UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Michael Okash, individually, and on behalf of those similarly situated, Plaintiff, v. Essentia Health, Defendant.	Case No. 0:23-cv-00482-JRT-LIB **SECOND AMENDED CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiff Michael Okash ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his attorneys of record, asserts the following against Defendant, Essentia Health ("Essentia" or "Defendant") based upon personal knowledge and upon information and belief, and the investigation of counsel, which included, among other things, consultation with experts in the field of data privacy.

INTRODUCTION

1. Plaintiff brings this class action complaint on behalf of a class of persons impacted by Defendant's unauthorized disclosure of their highly sensitive Personal Health Information ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information") to third parties. Defendant solicited and obtained Plaintiff's and the Class's Sensitive Information as part of its ordinary business activities as a medical services provider.

2. Defendant provides patients and prospective patients with an online website, essentiahealth.org, to *inter alia*, find doctors or providers[1], inquire about scheduling appointments[2] and schedule appointments[3], search for services[4], find a facility[5], research information related to medical issues and conditions[6] or medications[7], including the location of pharmacies, review accepted insurance[8], and research assistance plans for paying medical bills and options for paying medical bills, including how to review your bill online.[9]

3. While using essentiahealth.org, patients, prospective patients, and website users, like Plaintiff and the proposed Class members, can research specific doctors and healthcare providers, services and specialties, and symptoms and conditions. Before the

[1] https://www.essentiahealth.org/find-doctor-provider/ (last visited Apr. 18, 2024).
[2] https://www.essentiahealth.org/patients-visitors/make-an-appointment/ (last visited Apr. 18, 2024).
[3] Schedule Online: Primary Care, Schedule an Appointment, https://www.essentiahealth.org/schedule-online/ (last visited Apr. 19, 2024) (The patient or prospective patient answers several questions about the appointment she is seeking and after several questions, the patient can select a date and time for appointment. The final page in the process of selecting an appointment states, "Thank you for scheduling your [Visit] with your health care team" and information displayed includes doctor name, date and time of appointment, time to arrive for appointment, and location of appointment. The appointment is reserved for the patient or prospective patient, "This time slot is reserved for you until […]" This is completed on essentiahealth.org).
[4] https://www.essentiahealth.org/services/ (last visited Apr. 19, 2024).
[5] https://www.essentiahealth.org/find-facility/ (last visited Apr. 18, 2024).
[6] https://www.essentiahealth.org/conditions-search/ (last visited Apr. 18, 2024).
[7] https://www.essentiahealth.org/services/pharmacy/get-your-prescription/ (last visited Apr. 18, 2024).
[8] https://www.essentiahealth.org/patients-visitors/billing/insurance-we-accept/ (last visited Apr. 18, 2024).
[9] https://www.essentiahealth.org/patients-visitors/billing/pay-a-bill/ (last visited Apr. 18, 2024).

website will let a website user search for doctors, facilities, or symptoms and conditions, it requires the user to input location identifying information.

4. Defendant encourages its patients and prospective patients to use its website to make the healthcare process "as comfortable and stress-free as possible." In doing so, Defendant represents to patients and prospective patients that its website is a secure platform, and the information provided, particularly healthcare information, will remain secure and confidential.

5. Recently, Plaintiff became aware that Defendant incorporates Meta Platform, Inc.'s ("Meta") tracking technology, the Meta Pixel ("Pixel"), on Essentia's website. Pixel is a snippet of code that, when embedded on a third-party website, tracks the prospective patient's activity on that website and then directly delivers that data to Meta. This includes tracking and logging pages and subpages the website user visits during a website session, clicks, searches and other submissions to the website, which in many cases includes sensitive personal, and identifying information that is not anonymized. Subsequent to information being communicated to and collected by the Pixel, Defendant utilizes the data gathered to build profiles for the purpose of future targeting and marketing, including ads posted directly on Essentia's website or on other websites. Here, the information transmitted to third-party Meta by Essentia, without Plaintiff's consent, most certainly included private healthcare information, which is some of Plaintiff's most personal and sensitive data.

6. The actions taken on Essentia's website, including all activities or movements website users take and all communications website users make while on

essentiahealth.org, are surreptitiously intercepted and tracked by the Meta Pixel and transmitted to Meta f/k/a Facebook, at the direction of Essentia.

7. Defendant's use of Pixel allowed for a broad scope of patient information, including highly confidential medical information, to be collected and transmitted to Meta without patients' knowledge or consent. Specifically, Pixel is designed to track website users' activity on a website or application. It can capture how visitors interact with the site, including buttons they click and information they provide to form fields or otherwise. When on a medically-focused website page like Essentia's website, these online activities (each captured by Pixel) reveal personal medical information, including, for example, Sensitive Information users input to schedule appointments with or research physicians, research specific ailments, or search for specific symptoms on the webpage, check insurance acceptance, and review facility and pharmacy locations. These are collectively known as "Website Communications."

8. After surreptitiously sharing Plaintiff's and other patients' information with Pixel, Defendant then, in violation of HIPAA, used that information to condition Pixel to improve and save costs on its marketing campaigns, improve its data analytics to increase revenue by, among other things, attracting new patients and expanding its services for existing patients.

9. As a result of Defendant's use of Pixel, Plaintiff's and the Class's Sensitive Information was collected and disclosed to third parties without authorization or consent and in violation of HIPAA. That information included: computer IP addresses; dates, times, and/or locations of appointments; information about patients' health care providers;

whether the individual was a patient or prospective patient; types of treatments or conditions researched; type of appointment or procedure scheduled with specific doctors; communications between patients and Essentia, which may have included first and last names and identifying record numbers; information about whether patients have insurance; gender, age, and sexual orientation; and if a patient had a proxy portal account, the name of the proxy, and other information submitted by Plaintiff and the Class on Defendant's website or application..

10. Such private information allows Meta to know that a specific patient or prospective patient was seeking confidential medical care or being treated for a specific condition.

11. Plaintiff and the Class never consented to, authorized, or otherwise agreed to allow Defendant to disclose their Sensitive Information to anyone other than those reasonably believed to be part of Defendant, acting in some medical care related capacity. Despite this, Defendant knowingly and intentionally disclosed Plaintiff's and the Class members' Sensitive Information to its vendors and other undisclosed third parties in violation of HIPAA and other laws.

12. The exposed Sensitive Information of Plaintiff and the Class members can and will likely be further exposed or disseminated to additional third parties who will utilize that data for retargeting or possibly to insurance companies utilizing the information to set insurance rates.

13. As a direct and proximate result of Defendant's unauthorized exposure of Plaintiff's and the Class's Sensitive Information, Plaintiff and the Class members have

suffered injury including an invasion of privacy, statutory damages, and the continued and ongoing risk to their Sensitive Information.

14. As such, Plaintiff and the Class bring this action to recover for the harm they suffered, and assert the following claims: Invasion of Privacy, Violation of the Minnesota Uniform Deceptive Trade Practices Act ("MUDPTA") (Minn. Stat. § 325D.43-48), Violation of Electronic Communications Privacy Act ("ECPA") (18 U.S.C. §§ 2511 & 2702), Violation of the Minnesota Wiretap Act (Minn. Stat. § 626A.02), Violation of the Minnesota Consumer Fraud Act (Minn. Stat. § 325F.69) and Unjust Enrichment.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interests or costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a different state from Defendant. This Court further has federal question jurisdiction pursuant to 29 U.S.C. § 1331 because this Complaint asserts claims pursuant to Defendant's violations of 28 U.S.C. § 2511.

16. This Court has jurisdiction over this action because Plaintiff is a resident and citizen of the State of Minnesota who received health care from Defendant while in the State of Minnesota. Defendant is a Minnesota corporation with its registered office located at 502 East Second Street, Duluth, MN 55805.

17. Venue is proper in this Court because Defendant's headquarters are located here, and Plaintiff's claims arise from Defendant's conduct in this District.

PARTIES

Plaintiff Michael Okash

18. Plaintiff Michael Okash is a natural person domiciled in the State of Florida. His permanent address is located in Florida. Since approximately 2000, Plaintiff spends approximately six months of each year (November through April) in Florida and six months of the year in Superior, Wisconsin (May through October). Plaintiff has visited Defendant's Superior, Wisconsin and Duluth, Minnesota medical facility locations.

19. Plaintiff receives medical services from Defendant every year, during May through October. It is Plaintiff's understanding that Defendant does not have clinics or offer in-person medical services in Florida.

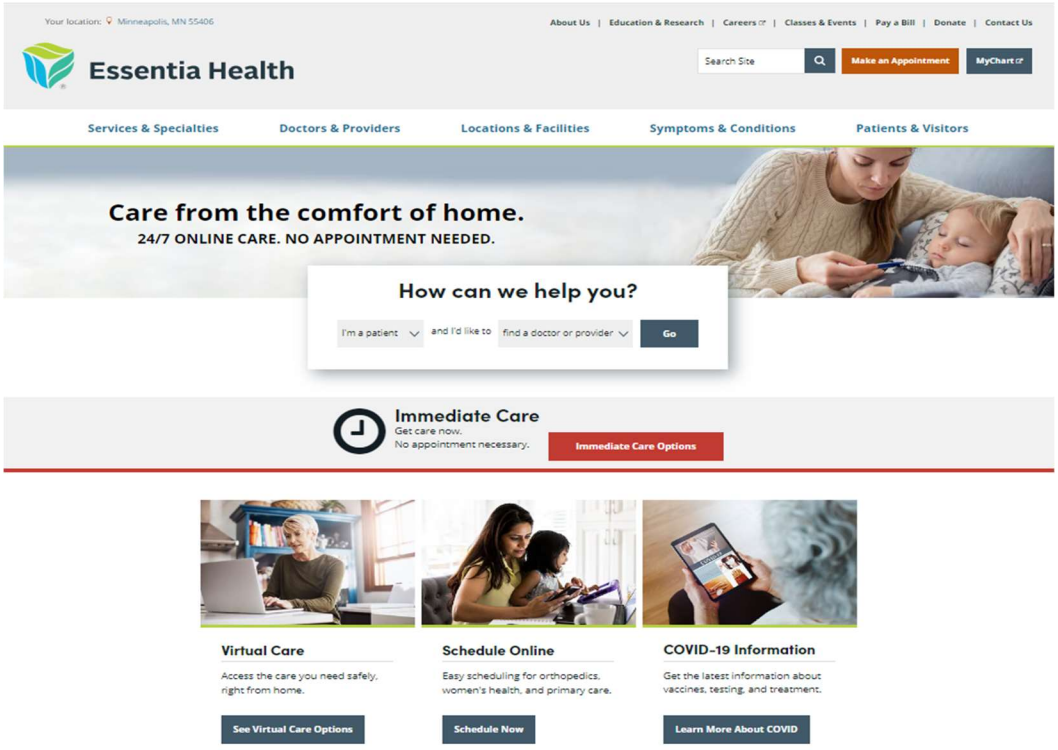
20. Plaintiff has visited www.essentia.org in connection with the medical services he received from Defendant, including visiting the public facing website while located in Florida, Wisconsin, and Minnesota and researched his prospective and ongoing medical care and treatment, including research related to specific physicians, locations for care, types of insurance accepted, and symptoms and conditions.

21. Plaintiff specifically recalls using essentiahealth.org, the public facing website, to research specific doctors and specialists that were referred to him, including Dr. Daniel Nikcevitch, and Dr. Nahi Kiblawi. Plaintiff's doctor-related research on essentiahealth.org included a search for the doctor, review of the doctor's credentials, specialties, and practice areas, and review of whether the doctor accepted Plaintiff Okash's medical insurance. Plaintiff researched all of his medical providers in the same manner, looking for information related to the provider's specialties, practice areas, credentials, and

insurance accepted. The contents of these searches that Plaintiff conducted as both a prospective Essentia patient and a current Essentia patient were all disclosed by Essentia to Meta through the Meta Pixel.

22. Below are screenshots from essentiahealth.org depicting an example of how Plaintiff researched one of his Essentia physicians, Dr. Nikcevich. In or around February 2022, Plaintiff did this research and communicated all of this information related to his past, present, and future medical care without logging into Essentia's patient portal. Dr. Nikcevich's's Essentia website profile page indicates he practices oncology and hematology.

23. **Step 1:** Navigated to www.essentiahealth.org. [10]

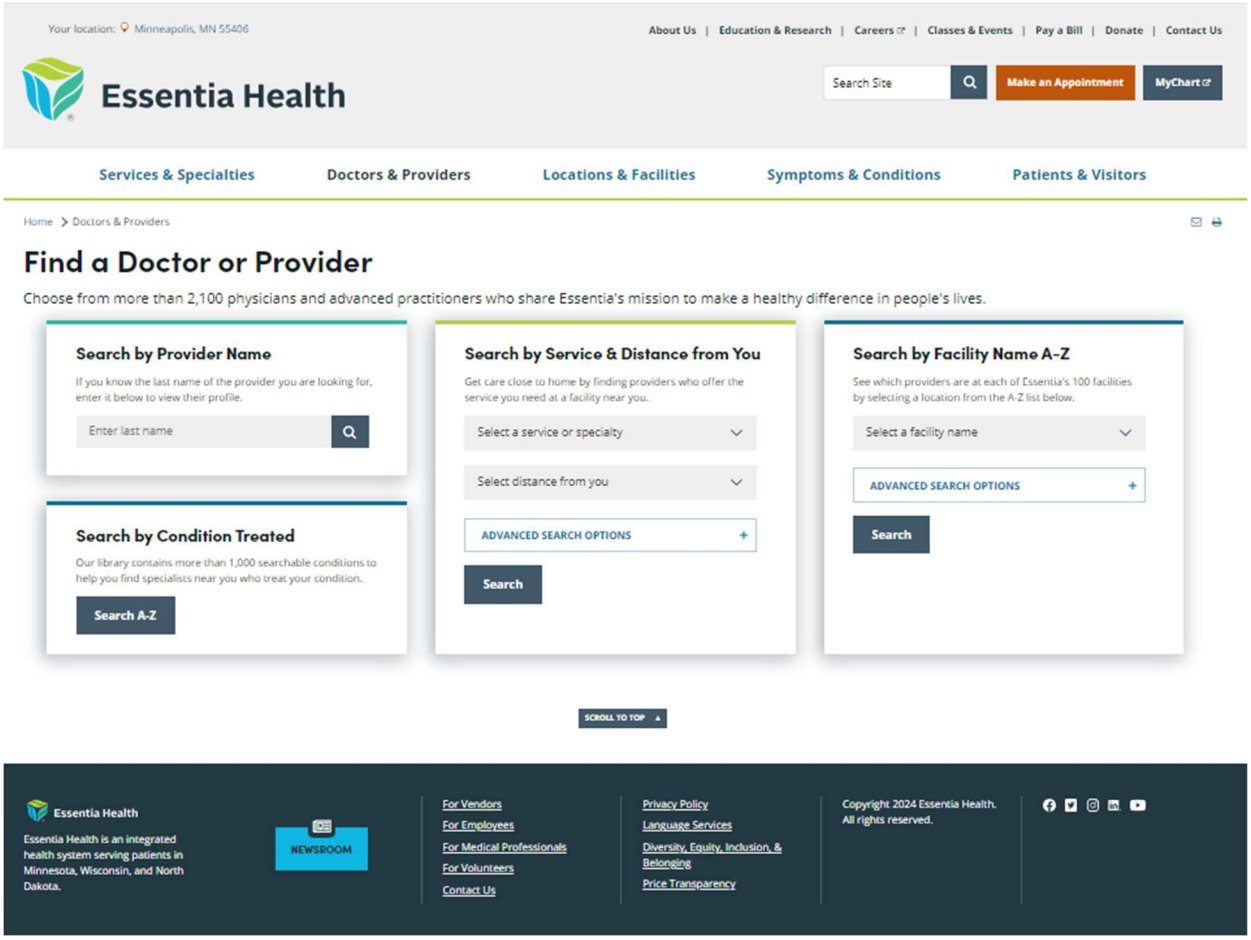


[10] Essentia Health website homepage, https://www.essentiahealth.org/ (last visited Apr. 16, 2024).

As demonstrated in this screenshot from essentiahealth.org, patients and prospective patients can use Defendant's homepage to inquire about "Virtual Care," "Schedul[ing] Online," and "COVID-19 Information." On Defendant's homepage, essentiahealth.org, patients can identify as a patient through the "I am a patient prompt." Patients or prospective patients can also identify their purpose for using the website through the "I'd like to" prompt, which includes options for finding a doctor or provider, searching for services, finding a facility, making an appointment, searching by condition, logging into MyChart, refilling a prescription, requesting medical records, paying a medical bill, and finding classes and events.

24. While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash visited Essentia's healthcare related website was disclosed by Essentia to Meta.

25. **Step 2:** Clicked on the "Doctors or Providers" page. Plaintiff Okash recalls conducting his search for Dr. Nikcevich by clicking on the "Doctors & Providers" page. [11]



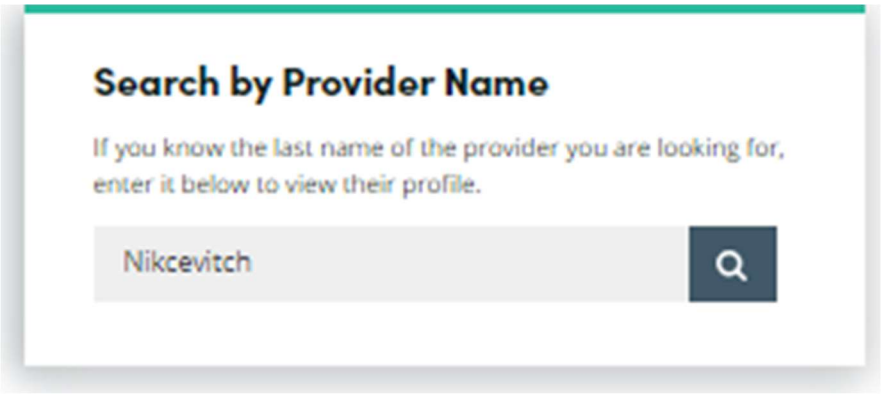
While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash visited Essentia's "Doctors & Providers" page to search for a physician was disclosed by Essentia to Meta.

a. On the "Doctors or Providers" page, patients and prospective patients can find doctors by searching by the provider's name, the condition treated, the service and location, or the facility name. Plaintiff Okash recalls

[11] Essentia Health Find a Doctor or Provider, https://www.essentiahealth.org/find-doctor-provider/ (last visited Apr. 16, 2024).

searching by the provider's name, as he was researching Dr. Nikcevich after a referral. The fact that Plaintiff Okash searched for Dr. Nikcevich on Essentia's website as a patient or prospective patient of that doctor was disclosed by Essentia to Meta.

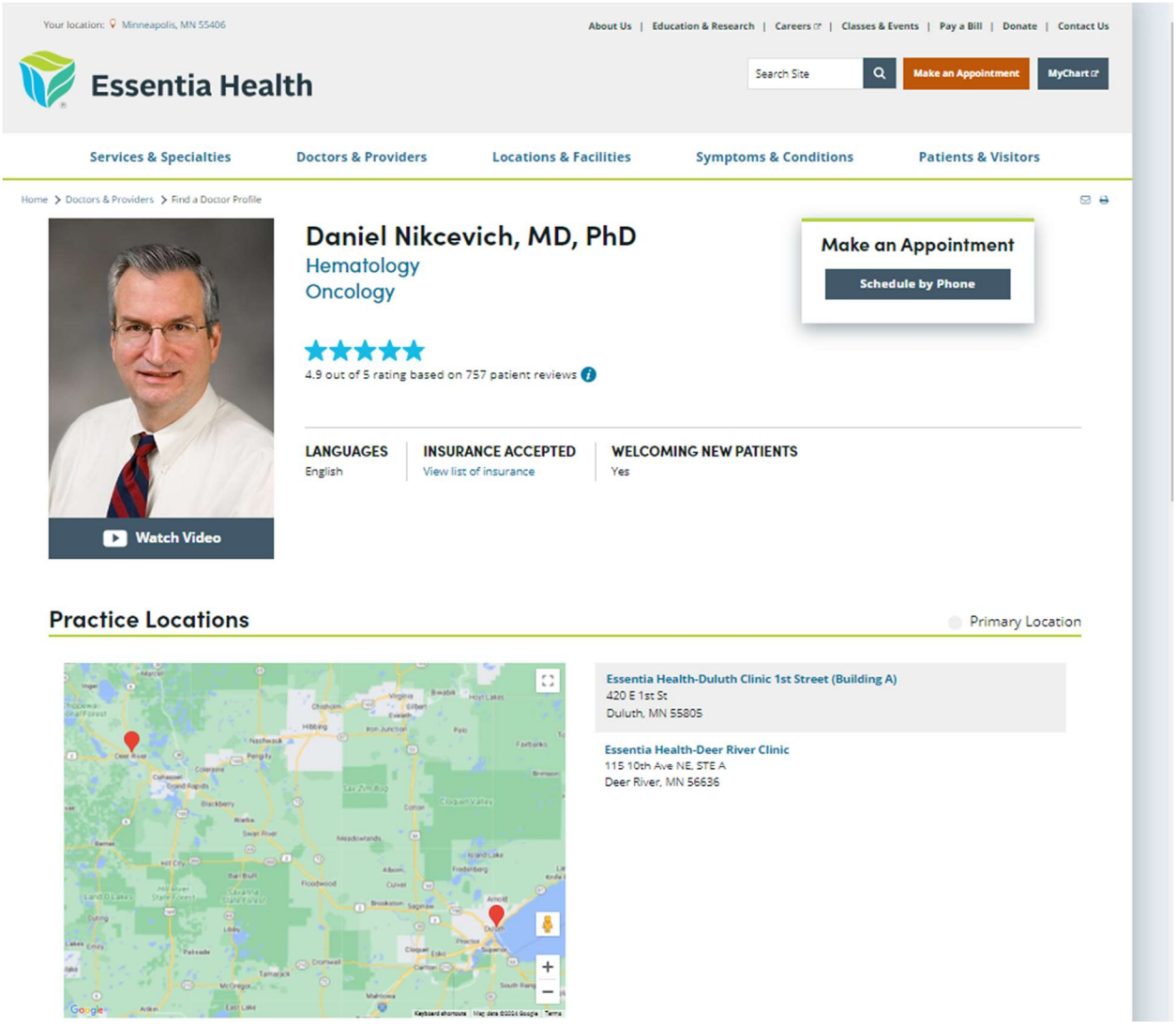
26. **Step 3:** Typed "Nikcevich" into the "Search by Provider Name" search box and submit by clicking the search button. The Search by Provider option is displayed below.[12]



27. While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash searched for Dr. Nikcevich on Essentia's website as a patient or prospective patient of that doctor was disclosed by Essentia to Meta.

[12] *Id.*

28. **Step 4:** Reviewed Find a Doctor Profile for Daniel Nikcevich, MD, PhD, including scrolling through the page to review "Conditions Treated" and "Education & Certifications." Dr. Nikcevich's doctor profile page is displayed below. [13]



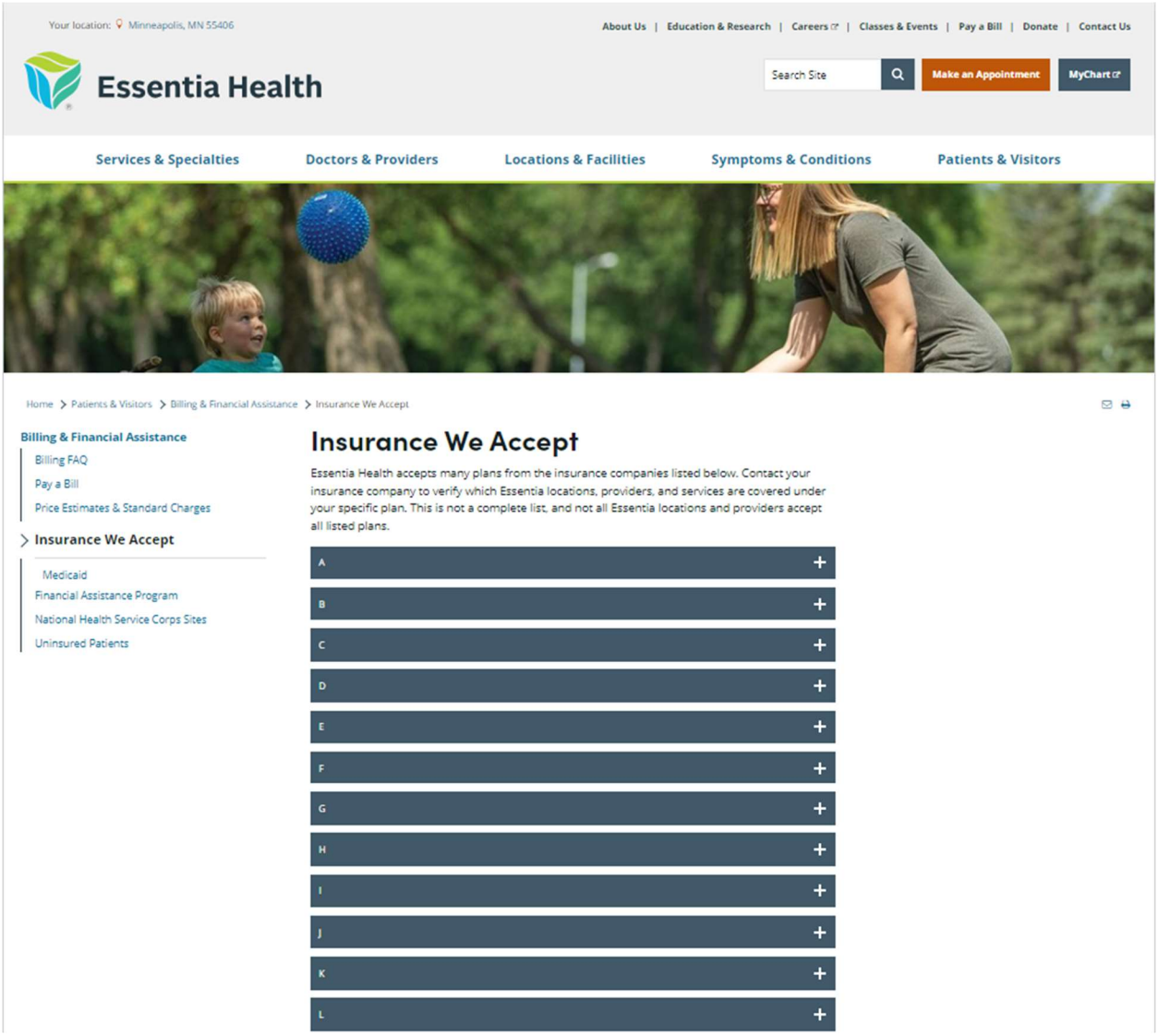
While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash conducted this analysis and research was disclosed by Essentia to Meta.

[13] Find a Doctor Profile: Daniel Nikcevich, MD, PhD, https://www.essentiahealth.org/find-doctor-provider/profile/daniel-nikcevich/ (last visited April 16, 2024).

a. On the first part of this profile, a patient or prospective patient can review the doctor's specialties. Here, those specialties include Hematology and Oncology. If a patient or prospective patient clicked on one of the specialties, that communication would be disclosed by Essentia to Meta. This means Meta would learn a specific person inquired about a specific Essentia doctor and the specific condition that doctor treats and for which the patient or prospective patient was seeking care. Plaintiff Okash cannot recall whether he clicked on "Oncology" from Dr. Nikcevich's doctor profile. Plaintiff does recall, however, researching Oncology on Essentia's website, and those communications were disclosed by Essentia to Meta.

b. On the doctor profile page, the patient or prospective patient can also review the doctor's rating based on patient reviews, the languages the doctor speaks, whether the doctor is welcoming new patients, and can click to schedule an appointment by phone. Plaintiff Okash reviewed these parts of Dr. Nikcevich's profile.

c. Specifically, Plaintiff Okash reviewed the "Insurance Accepted" by clicking the link and reviewing the "Insurance We Accept" page, displayed below.[14]



While Essentia utilized Meta Pixel, the fact that Plaintiff Okash reviewed the insurance Essentia accepts was disclosed by Essentia to Meta.

[14] Essentia's Insurance We Accept, https://www.essentiahealth.org/patients-visitors/billing/insurance-we-accept/ (last visited Apr. 16, 2024).

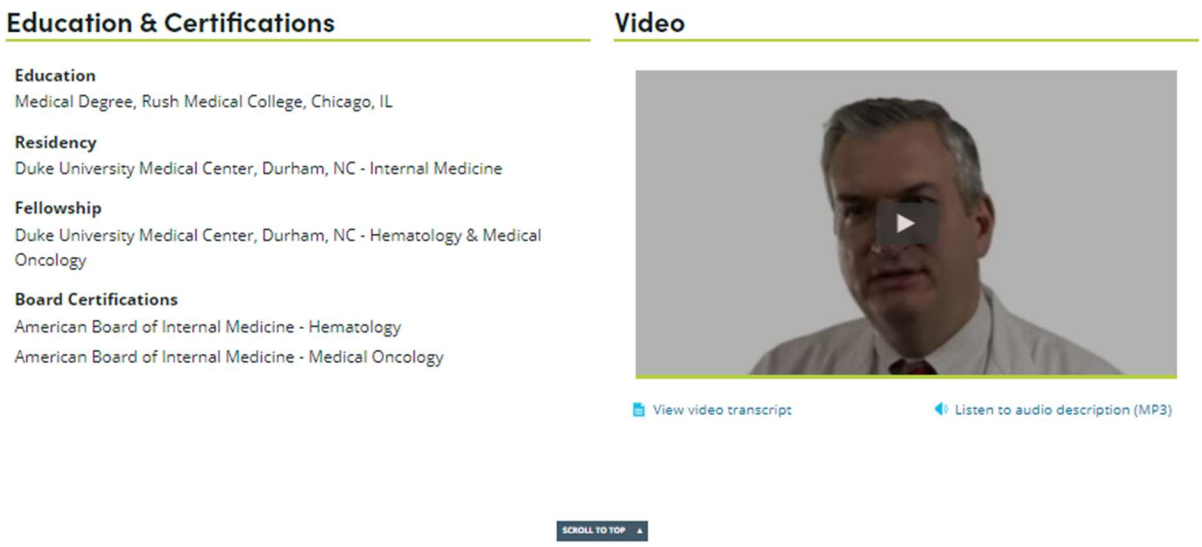
d. Plaintiff recalls scrolling through Dr. Nikcevich's doctor profile to review the "Conditions Treated" section. This part of the doctor profile page is displayed below.[15]

Conditions Treated

Anal cancer	Anemia	Bladder cancer
Blood cancer	Blood clot	Blood disorders
Bone cancer	Bone marrow disorders	Brain cancer
Brain tumor	Breast cancer	Cancer
Carcinoid tumors	Cervical cancer	Colon cancer
Deep vein thrombosis	Esophageal cancer	Gallbladder cancer
Head and neck cancer	Hematologic cancer	Hemophilia
Hodgkin's lymphoma	Hypercalcemia	Immune thrombocytopenic purpura
Kidney cancer	Leukemia	Leukemia (myeloid)
Leukocytosis	Liver cancer	Lung cancer
Lymphoma	Melanoma	Myelodysplastic syndromes
Myeloma	Myeloproliferative disorders	Neuroendocrine tumors
Neutropenia	Non-hodgkin's lymphoma	Ovarian cancer
Pancreatic cancer	Pancytopenia	Polycythemia rubra vera
Prostate cancer	Rectal cancer	Sarcoma
Skin cancer	Stomach cancer	Testicular cancer
Uterine cancer		

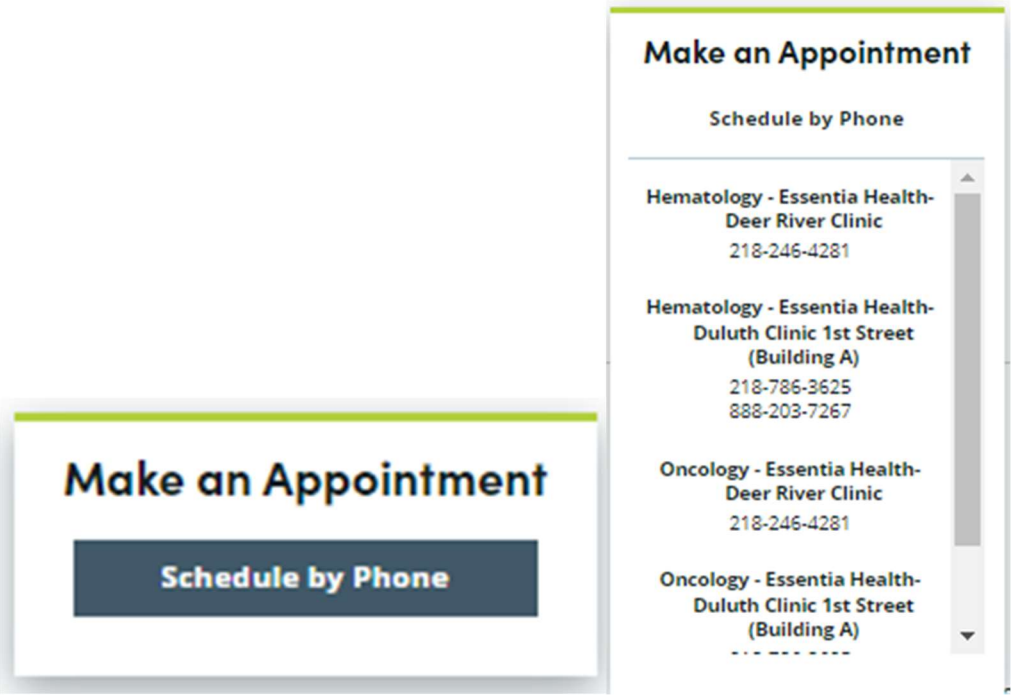
[15] *Id.*

e. Plaintiff Okash recalls scrolling through Dr. Nikcevich's doctor profile to review the "Education & Credentials" section. This part of the doctor profile page is displayed below.[16]



[16] *Id.*

29. **Step 5:** Clicked the "Schedule by Phone" button to "Make an Appointment. The fact that a patient or prospective patient clicked the "schedule by phone" button on Essentia's website would be disclosed by Essentia to Meta. The "Schedule by Phone" button and the display after clicking that button are both displayed below.[17, 18]



30. Plaintiff communicated with Essentia and provided his information as outlined in steps one through five above without ever logging into his patient portal. These communications disclose that Plaintiff Okash was interested in care from a specific Essentia doctor, Dr. Daniel Nikcevich, an oncology and hematology specialist. Plaintiff's Website Communications may have also disclosed the specific kind of care Plaintiff sought from Dr. Nikcevich, including oncology, which Plaintiff certainly communicated on other pages of Essentia's website. Plaintiff conducted the same searches for his other Essentia

[17] *Id.*
[18] *Id.*

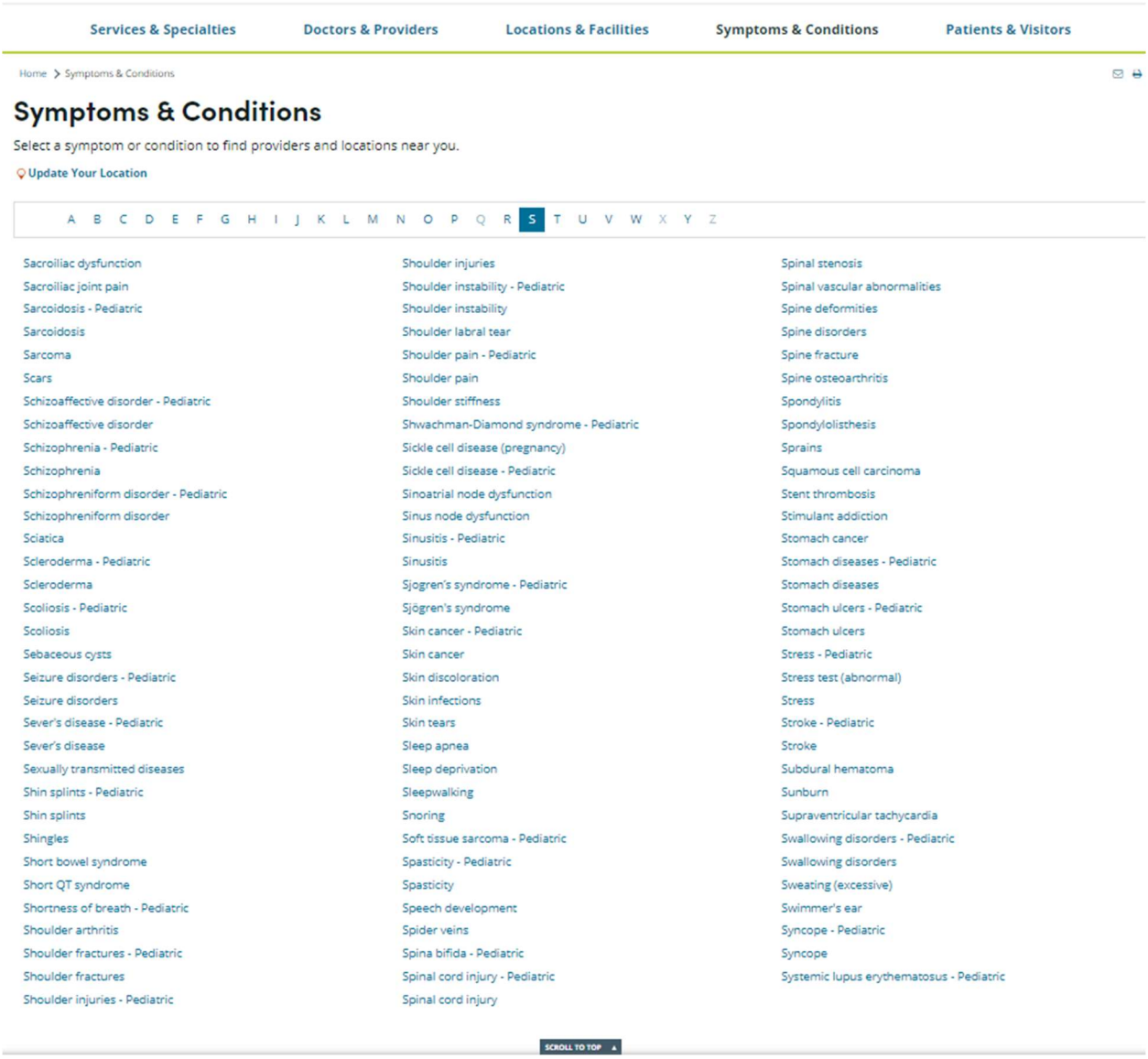
physicians, and this information was likewise disclosed by Essentia to Meta.

31. Plaintiff Okash also researched his specific medical conditions and treatments for the purposes of better understanding the type and quality of care Essentia could provide him. Okash's Website Communications on Essentia's website included searching for and disclosing specific medical diagnosis while on the website, such as his sleep apnea, bladder cancer, and diabetes.

32. When an Essentia patient or prospective patient, like Plaintiff Okash searches for a symptom or condition, they are prompted to distinguish between care from a primary care provider or a specialist. Upon selection of either a primary care provider or specialist, the website user is directed to a page that lists locations where, based upon that user's location, the individual can receive care for that symptom or condition from Essentia.

33. An example of a search for sleep apnea, like the one Plaintiff Okash conducted on essentiahealth.org, is outlined below through website screenshots.

34. **Step 1**: Go to the "Symptoms and Conditions" Page, which is depicted below. [19]



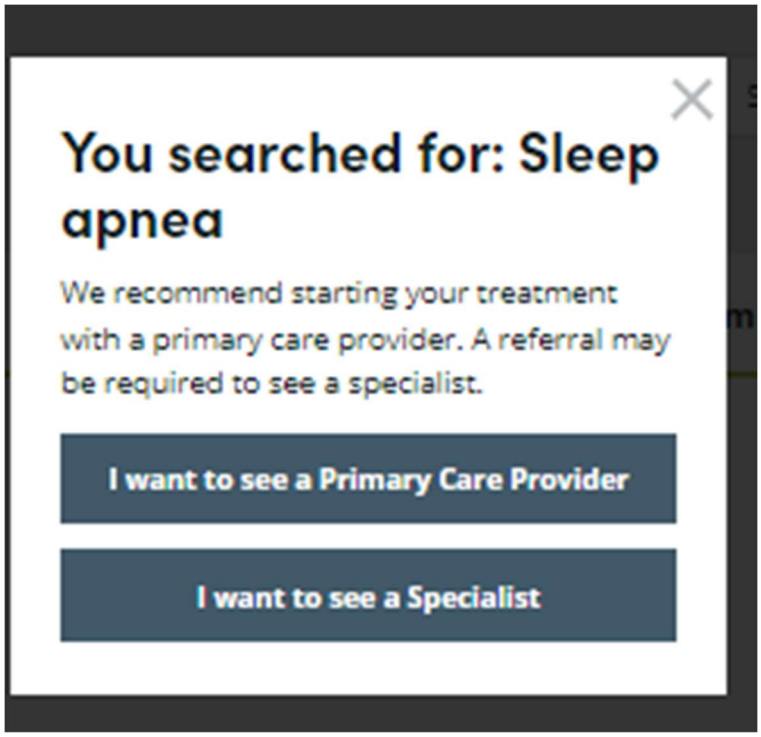
This page lists various symptoms and conditions in alphabetical order. While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash or an Essentia patient or prospective patient used this page to look at symptoms and conditions was disclosed by Essentia to

[19] Essentia Symptoms and Conditions, https://www.essentiahealth.org/conditions-search/ (last visited Apr. 16, 2024).

Meta.

35. **Step 2**: Select "Sleep Apnea." Plaintiff Okash recalls conducting a search for sleep apnea on Essentia's website. While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash or any other Essentia patient or prospective patient used this page to search for sleep apnea was disclosed by Essentia to Meta.

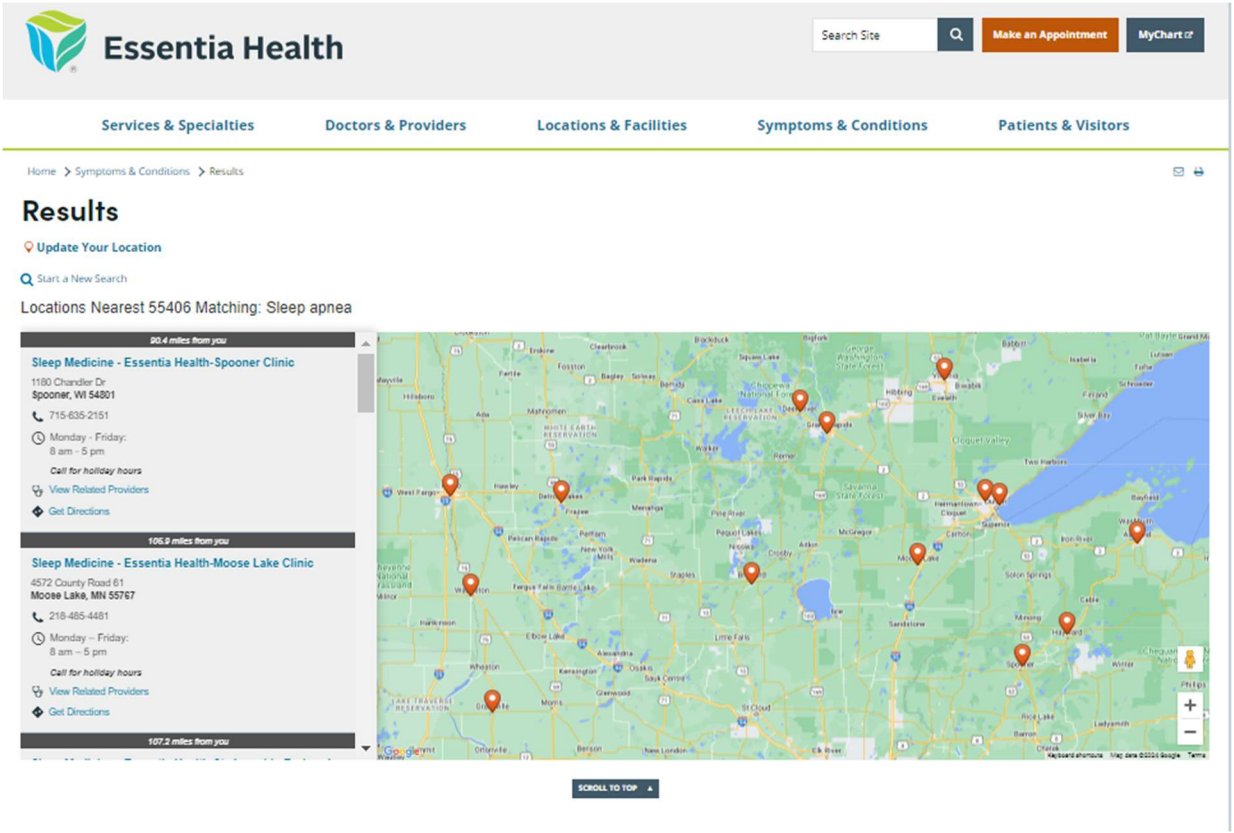
36. **Step 3:** Select "I want to see a Specialist." Plaintiff Okash typically seeks care from specialists, and recalls researching a sleep apnea specialist from Essentia for his disorder with intent to seek care for the disorder from an Essentia provider. [20]



While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash or any other Essentia patient or prospective patient used this page to search for sleep apnea specialist was disclosed by Essentia to Meta.

[20] *Id.*

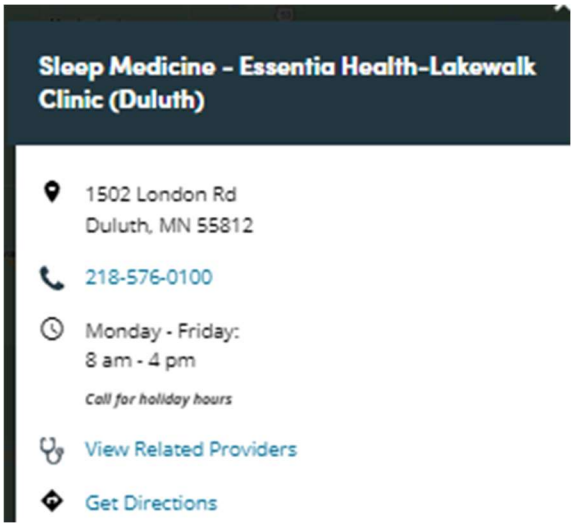
37. **Step 4:** Review the locations provided. Below are the locations Essentia offered a website user located in Minneapolis, Minnesota after that user selected "I want to see a Specialist." [21]

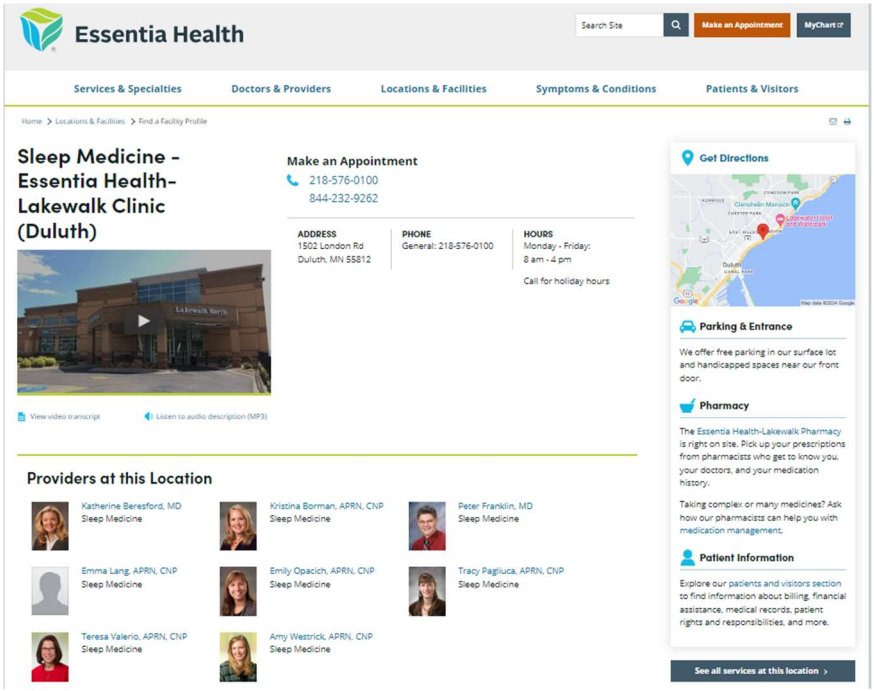


While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash or any other Essentia patient or prospective patient used this page to search for a sleep apnea specialist near a specific location was disclosed by Essentia to Meta.

[21] Search Results for Sleep Apnea, https://www.essentiahealth.org/conditions-search/results/?termId=3ce3d384-2484-e711-8108-001dd8b71c9e (last visited Apr. 16, 2024).

38. **Step 5:** Select specific location. For this example, Plaintiff Okash selected the Essentia Health-Lakewalk Clinic (Duluth). Below are the pages he would have been redirected to after selecting the Lakewalk location. [22, 23]





[22] *Id.*

[23] Find a Facility Profile, https://www.essentiahealth.org/find-facility/profile/sleep-medicine-essentia-health-lakewalk-clinic-duluth/ (last visited Apr. 15, 2024).

While Essentia utilized the Meta Pixel, the fact that Plaintiff Okash or any other Essentia patient or prospective patient used this page to search for sleep apnea specialist at a specific location was disclosed by Essentia to Meta.

39. To receive services from Defendant, Plaintiff had to provide personally identifying information and location information, along with other Sensitive Information. Defendant encouraged and recommended that Plaintiff utilize Defendant's online website to schedule appointments and to research medical conditions, services, providers, and facilities, among other things.

40. Plaintiff is a Facebook user and has had a Facebook account since at least 2007. After visiting essentiahealth.org, Plaintiff recalls receiving ads on Facebook for Essentia, and ads related to his medical care from Essentia. After using Defendant's website, Plaintiff recalls receiving targeted advertisements related to information he had researched while on Defendant's website. Indeed, Plaintiff Okash specifically recalls receiving ads related to a sleep apnea machine after he began receiving care from Essentia for his sleep apnea.

41. Plaintiff reasonably expected that his online communications with Defendant were between him and Defendant and that such communications would not be shared with third parties without his consent. Without Plaintiff's knowledge, consent, or authorization, Defendant exposed and intentionally allowed third-party Meta to intercept Plaintiff's personal, private, and confidential data through Meta Pixel.

42. Plaintiff had his Sensitive Information disclosed by Defendant's breach of his privacy and unlawful disclosure of his confidential and private health information.

Defendant Essentia

43. Defendant is a Minnesota corporation that is licensed to do business in the State of Minnesota and has a registered office located 502 East Second Street, Duluth, MN 55805.

FACTUAL BACKGROUND

A. Defendant Collected, Maintained, and Stored Sensitive Information

44. Defendant Essentia is an integrated health system serving patients in Minnesota, Wisconsin, and North Dakota. The company has approximately 15,000 employees, including 2,160 physicians and advanced practitioners who serve Defendant's patients and communities "through the mission of being called to make a healthy difference in people's lives."[24] Defendant has 4 hospitals, 77 clinics, six long-term care facilities, three assisted living facilities, three independent living facilities, six ambulance services, 24 retail pharmacies, and one research institute.[25]

45. To obtain healthcare services, patients and prospective patients, like Plaintiff and the Class, must provide Defendant with highly sensitive information, including PHI, PII, or both. Defendant compiles, stores, and maintains the highly sensitive PII and PHI and, often, through the provision of its services, creates records containing additionally highly sensitive data concerning patients' medical diagnostics, treatment, and other personal information documented by medical providers. Defendant serves hundreds of thousands of individuals every year, meaning it has created and maintains a massive

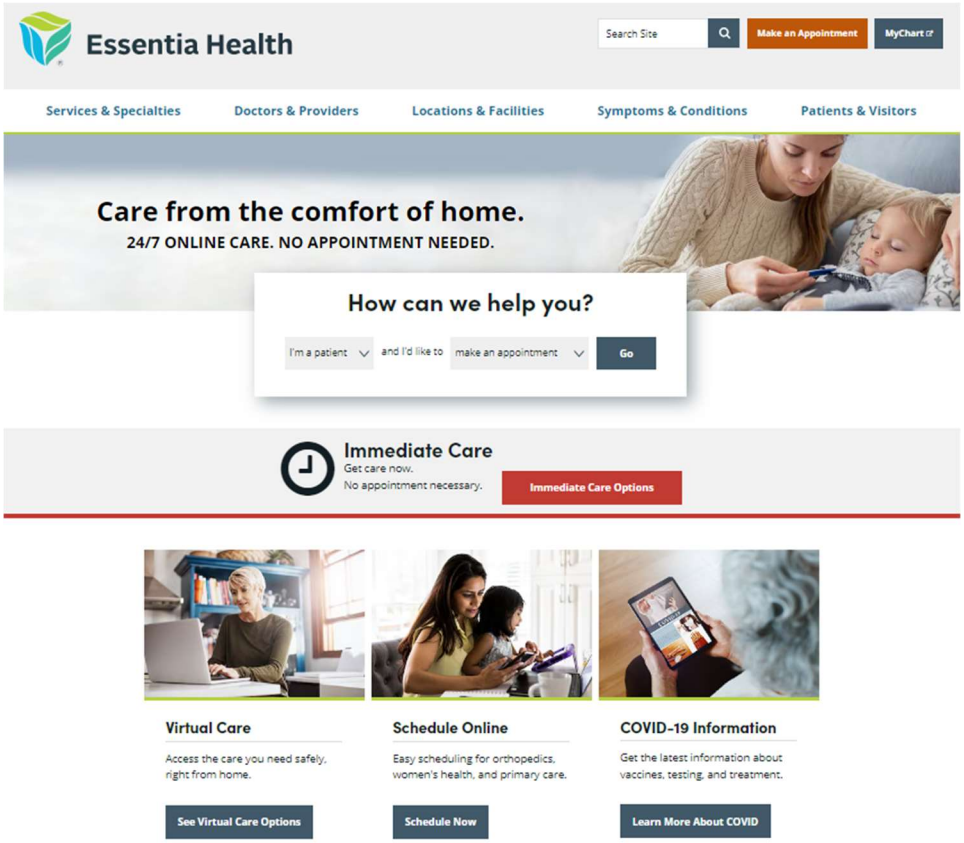
[24] About Us, https://www.essentiahealth.org/about/ (last visited April 15, 2024).
[25] *Id*.

repository of Sensitive Information.

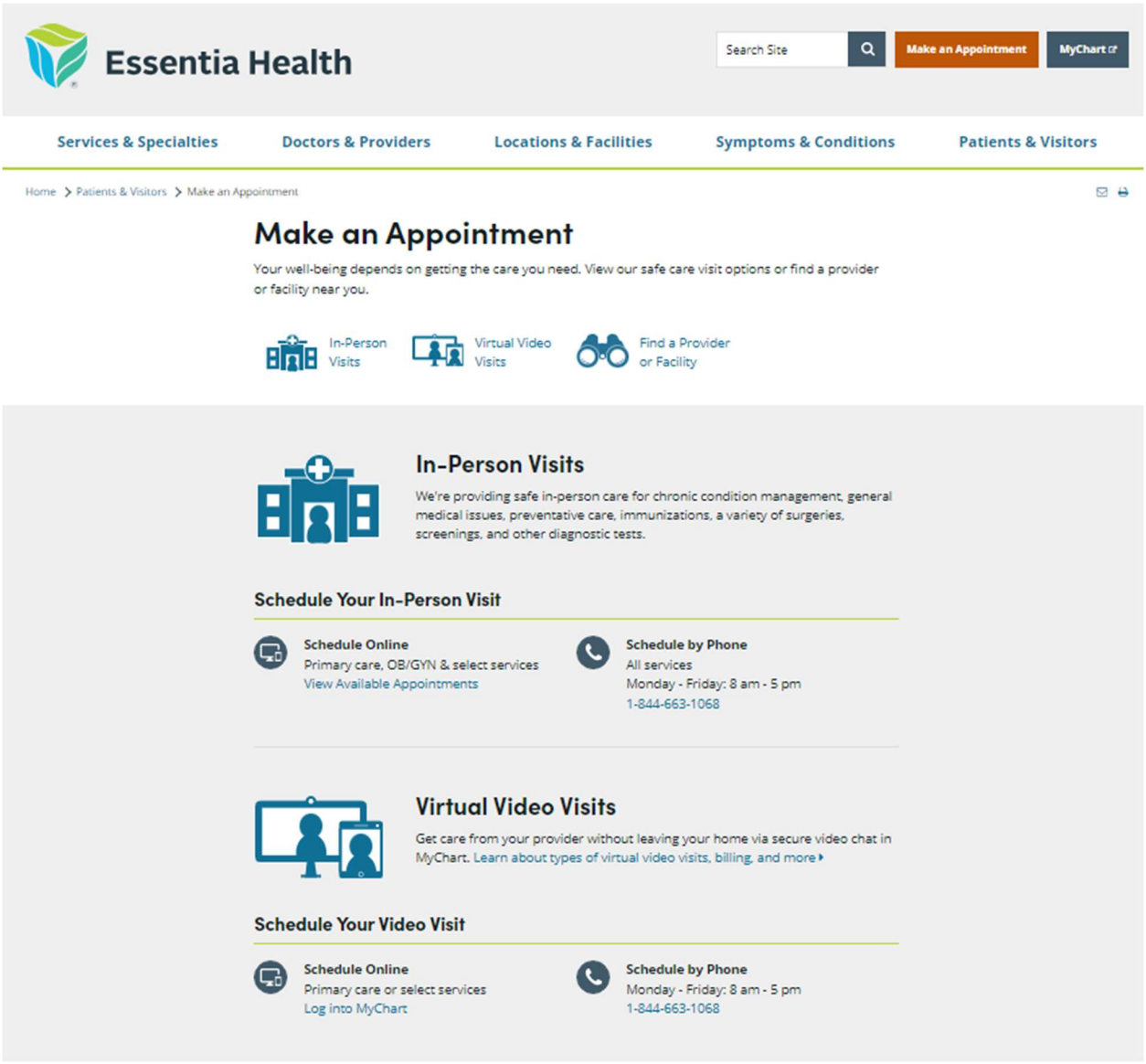
46. Defendant also collects massive amounts of sensitive, personal information from patients and prospective patients on its website, essentiahealth.org. For example, when a patient or prospective patient uses the website to schedule an appointment, before ever navigating to the MyChart page or logging into a patient MyChart account, Essentia collects vast amounts of Sensitive Information.

47. Below are several screenshots from Essentia's website demonstrating the types of information a patient or prospective patient information submits to Essentia to make an appointment for an adult annual physical.

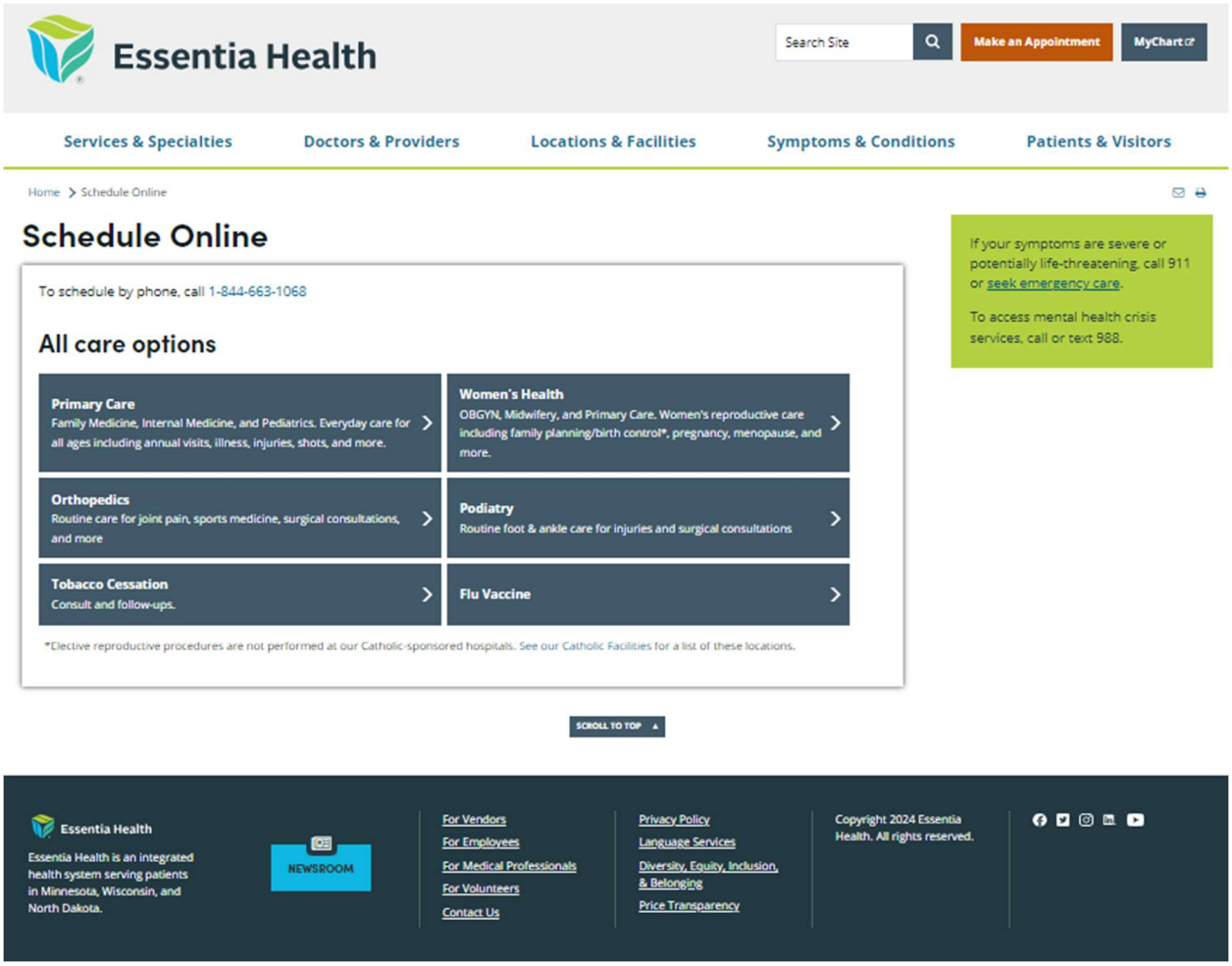
a. **Step 1:** Go to essentiahealth.org and select "I'm a patient" and I'd like to "make an appointment."



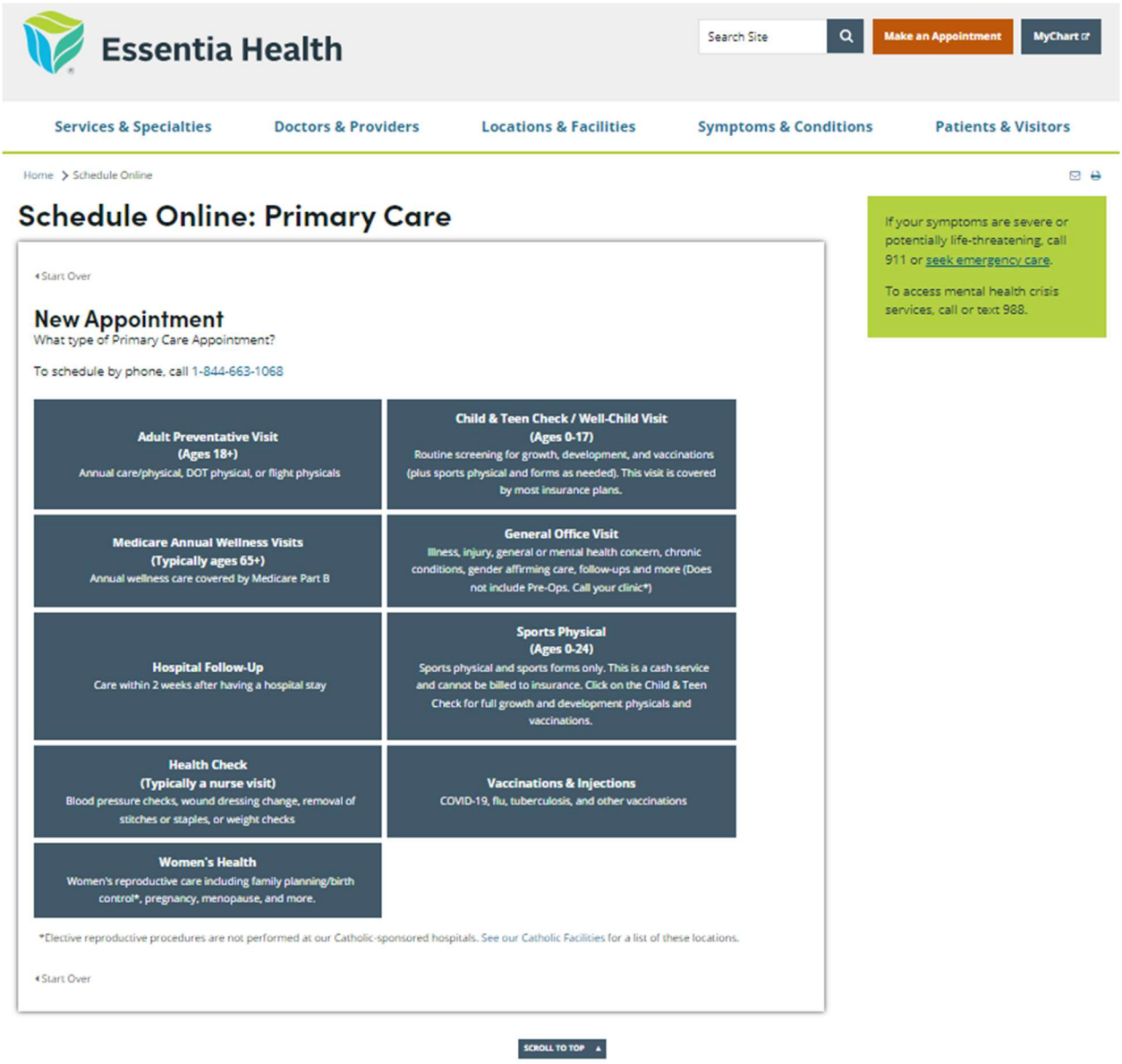
b. **Step 2:** Select "View Available Appointments" under the heading "Schedule Online."



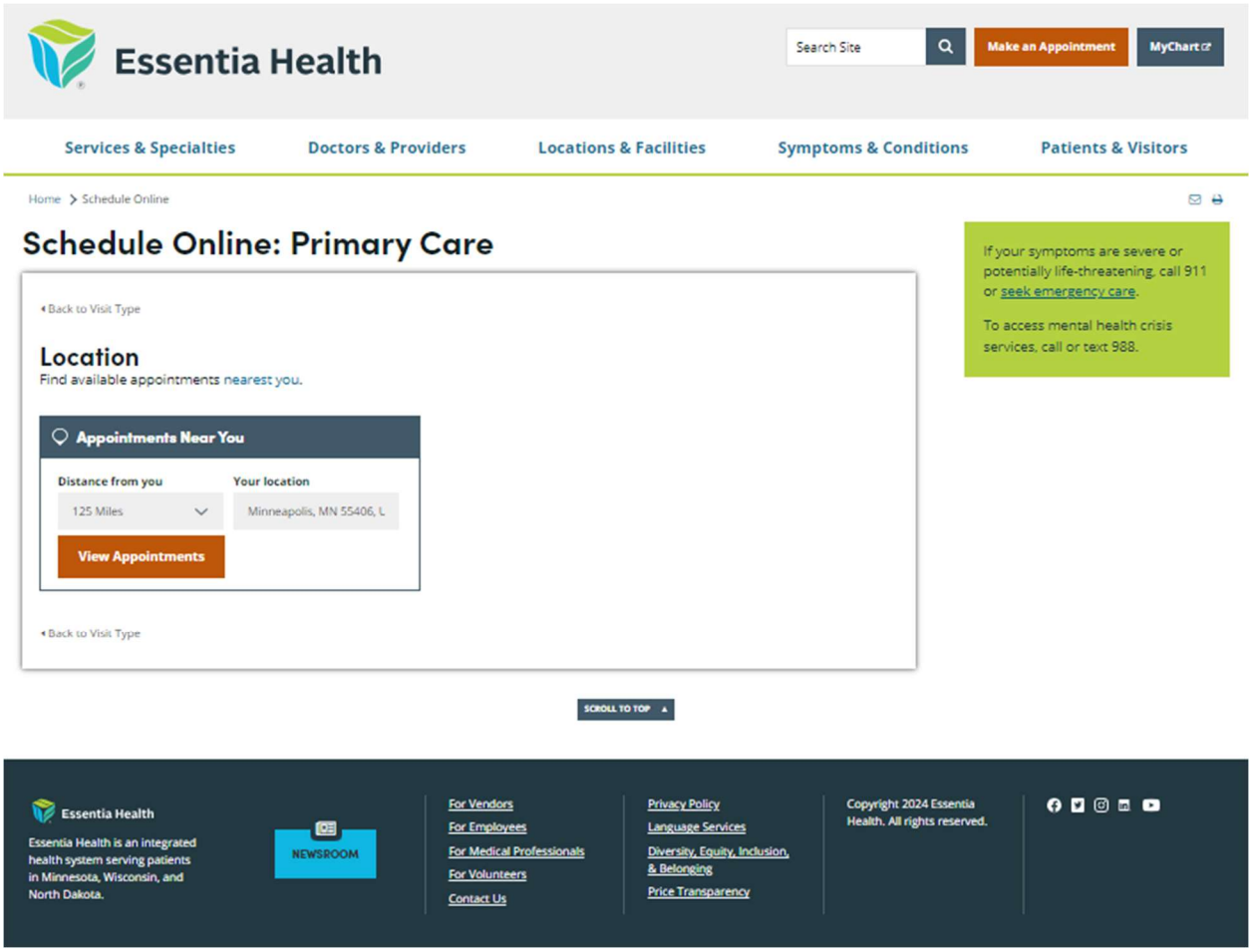
c. **Step 3:** Review "All Care Options" and select "Primary Care."



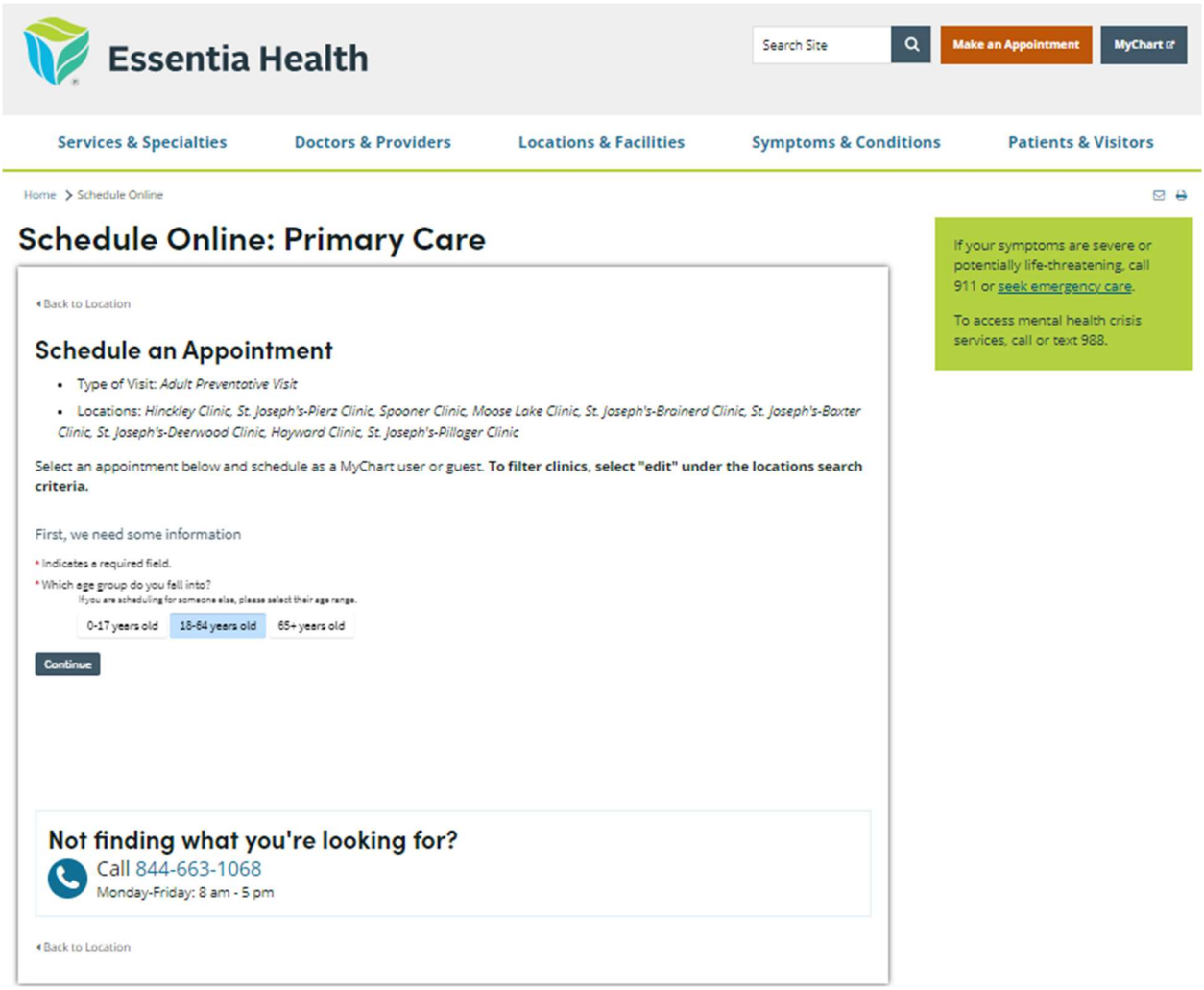
d. **Step 4:** Review the types of "Care Appointment[s]" and select "Adult Preventive Visit."



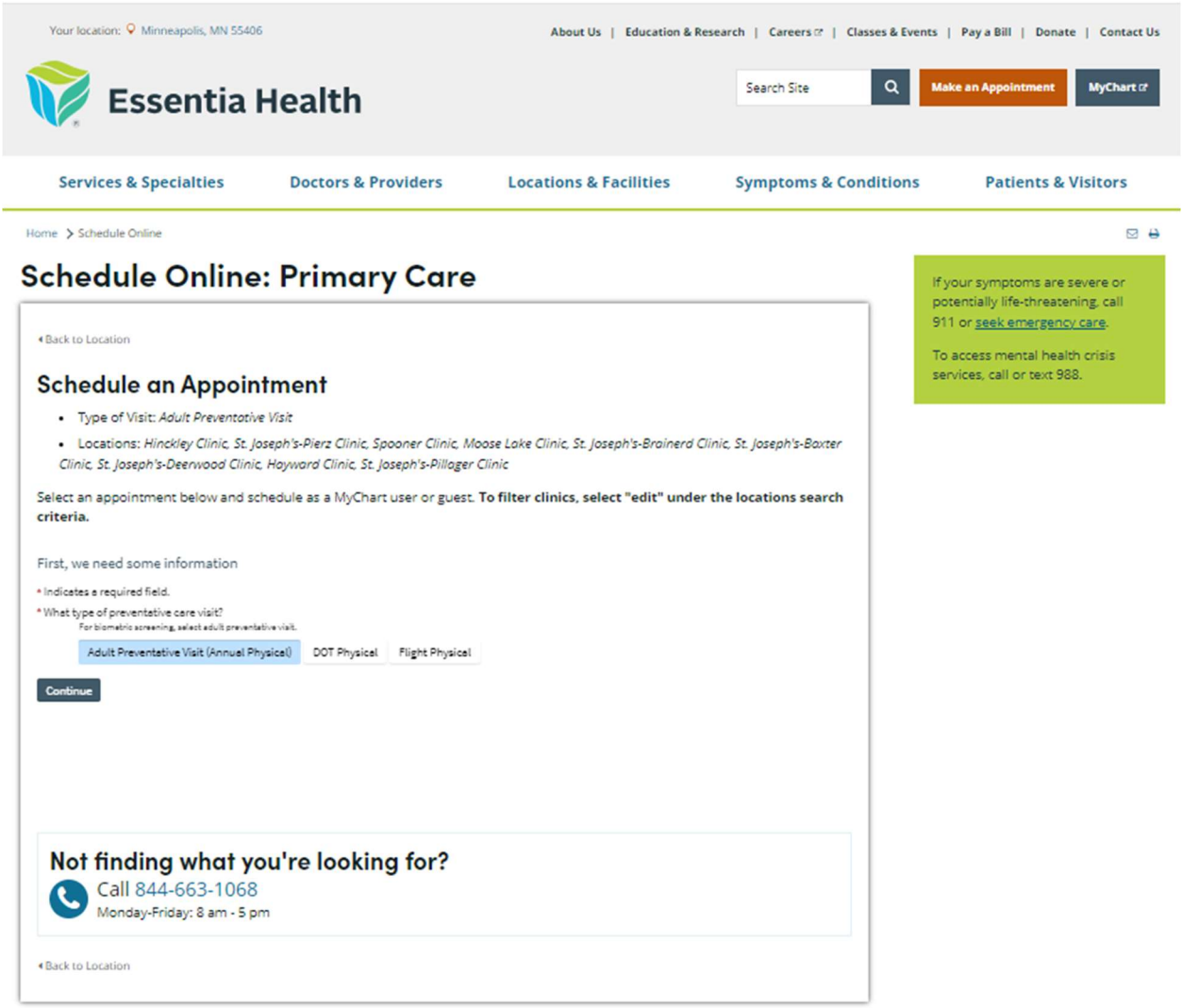
e. **Step 5:** Input Location Information and select "View Appointments."



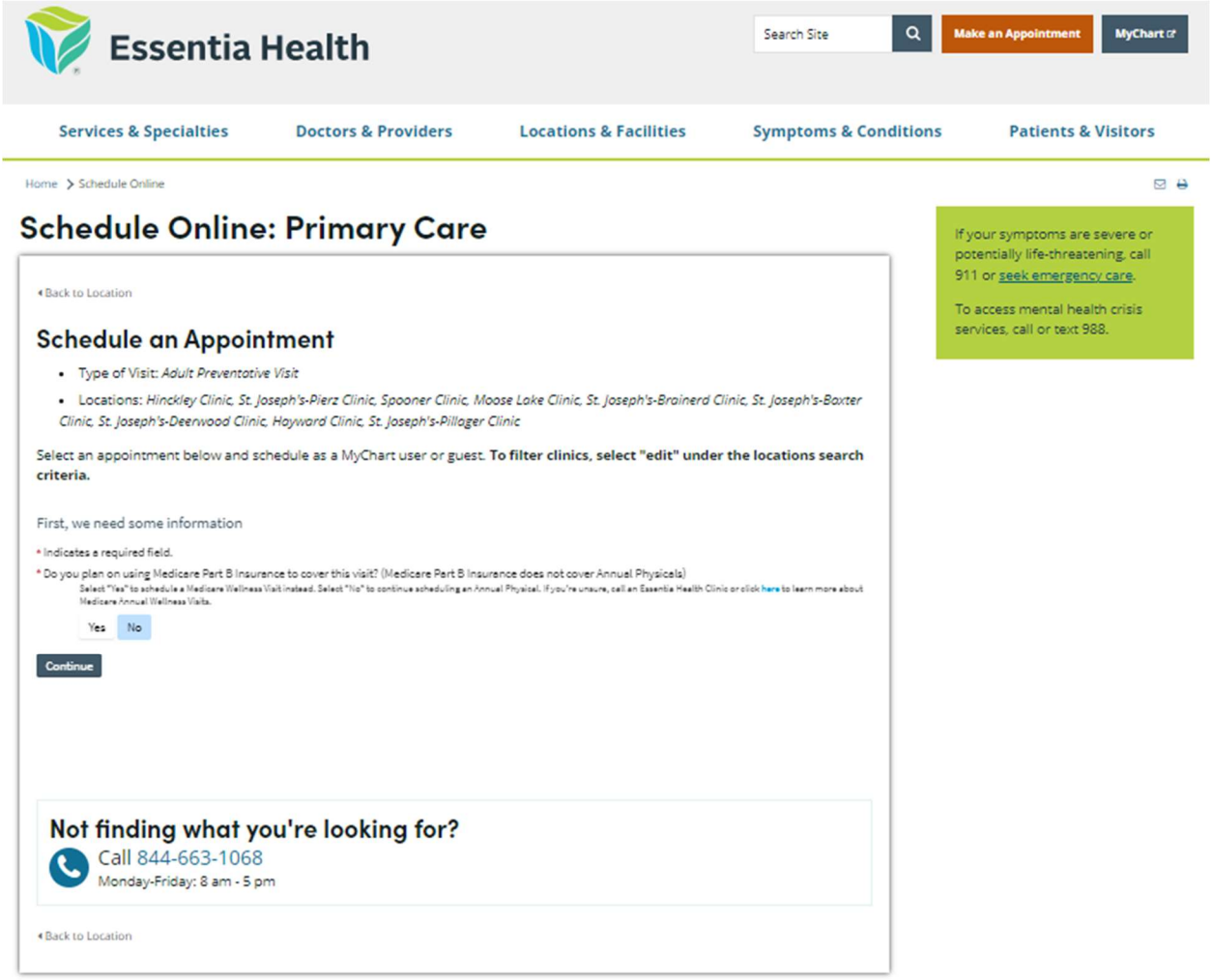
f. **Step 6:** Select the proper age range and click "Continue."



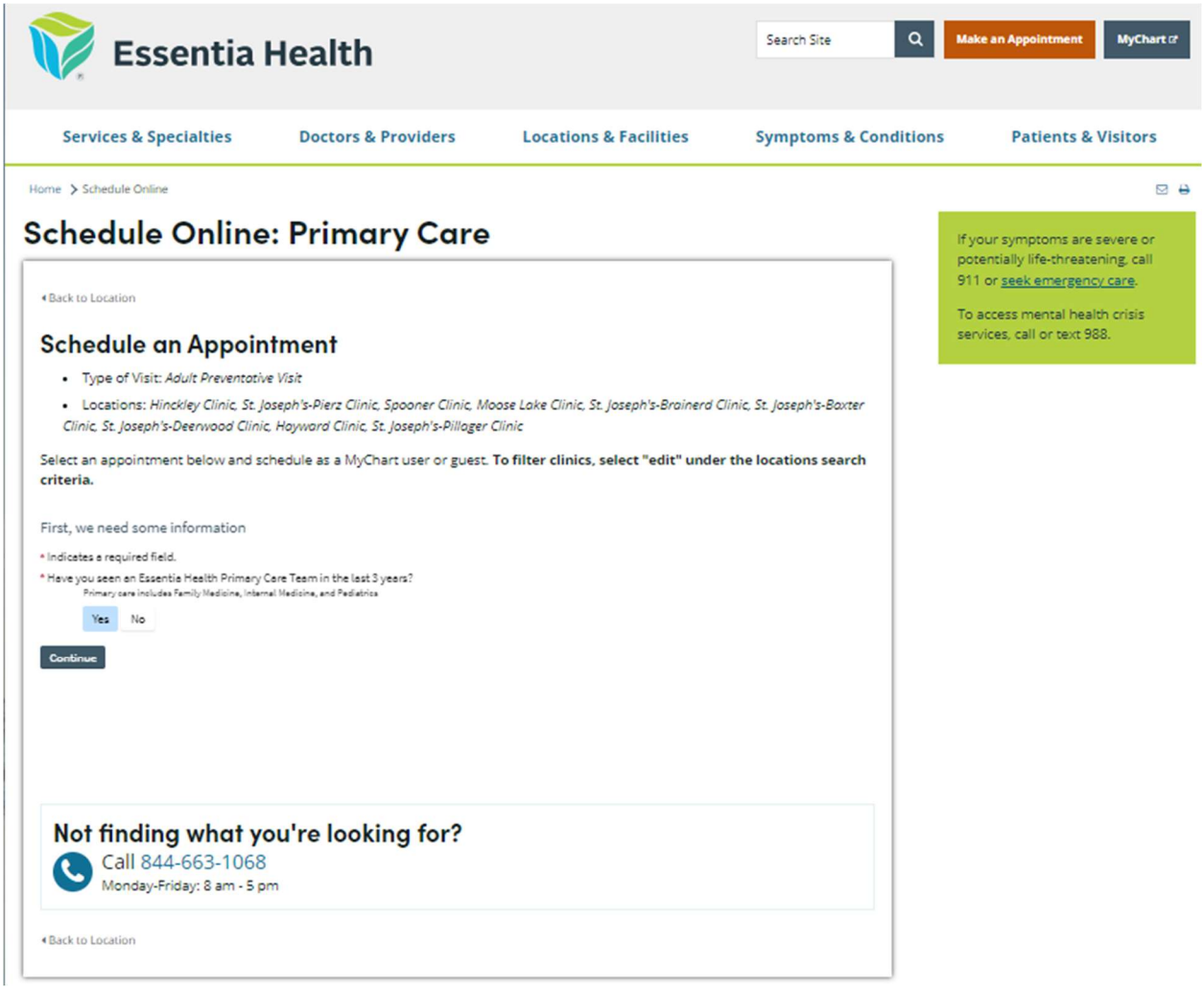
g. **Step 7:** Select "Adult Preventive Visit (Annual Visit) and click "Continue."



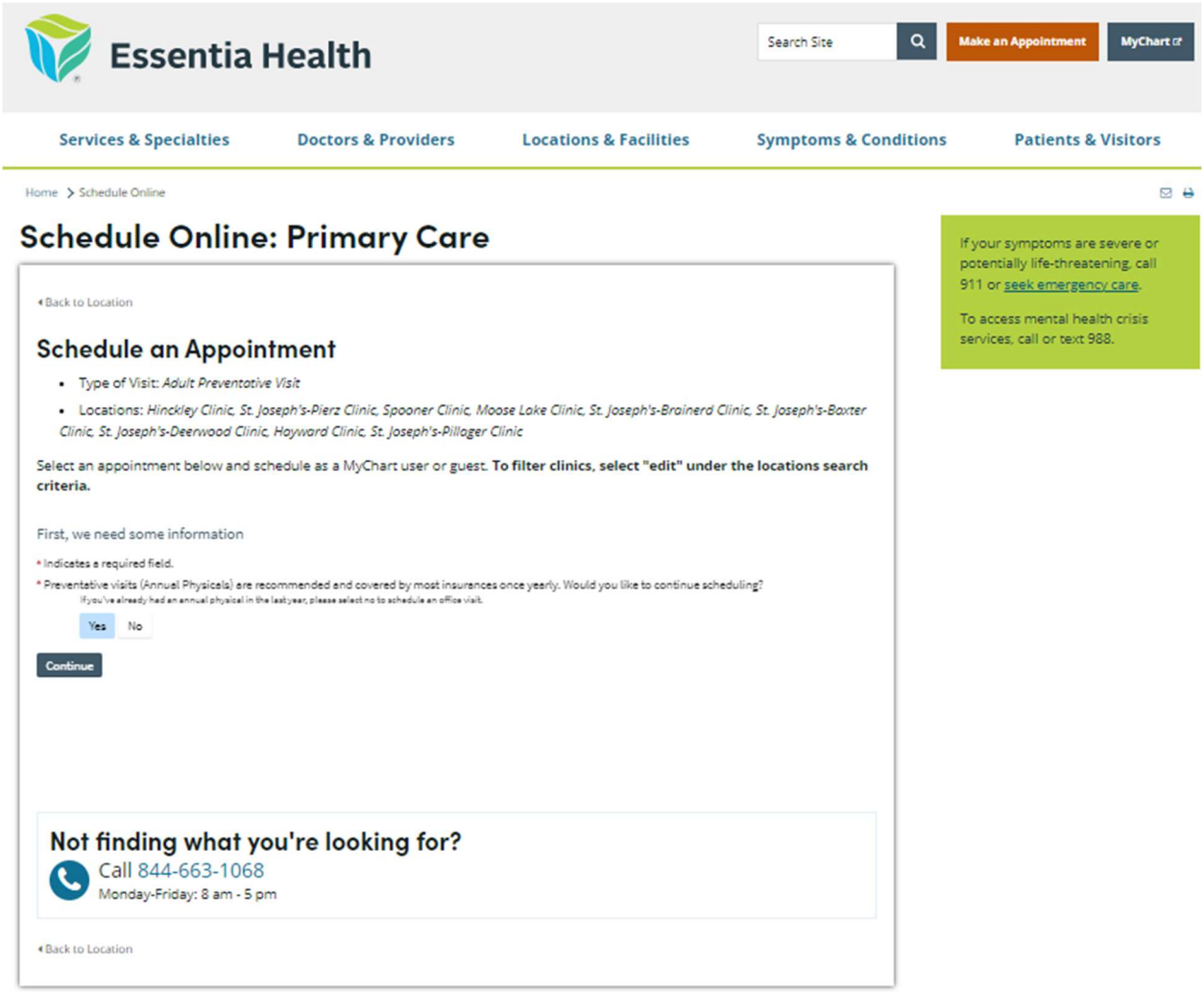
h. **Step 8:** Answer whether patient or prospective patient intends to use Medicare Part 5 insurance and select "Continue."



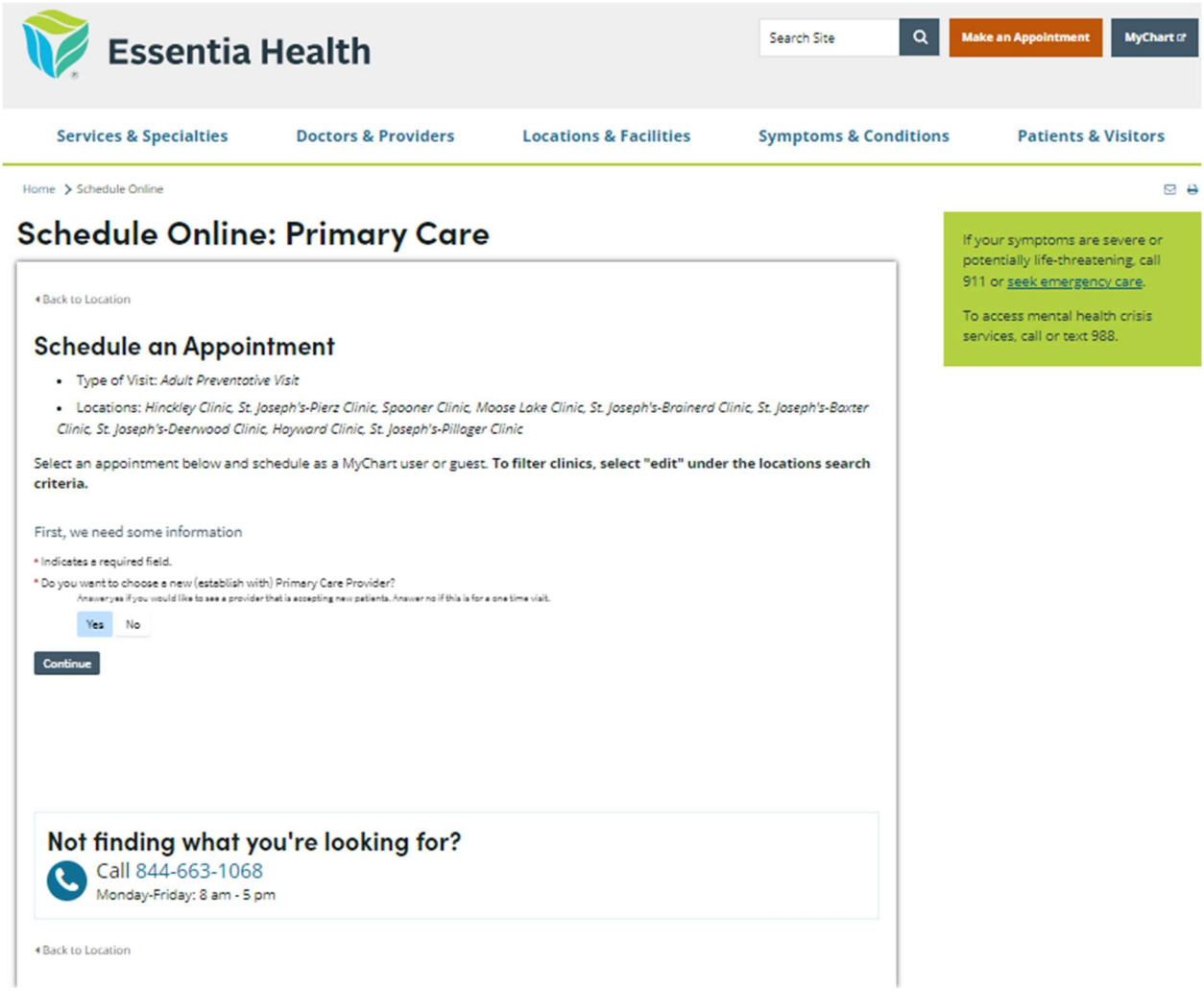
i. **Step 9:** Answer whether patient or prospective patient has been to an Essentia provider within the last 3 years and click "Continue."



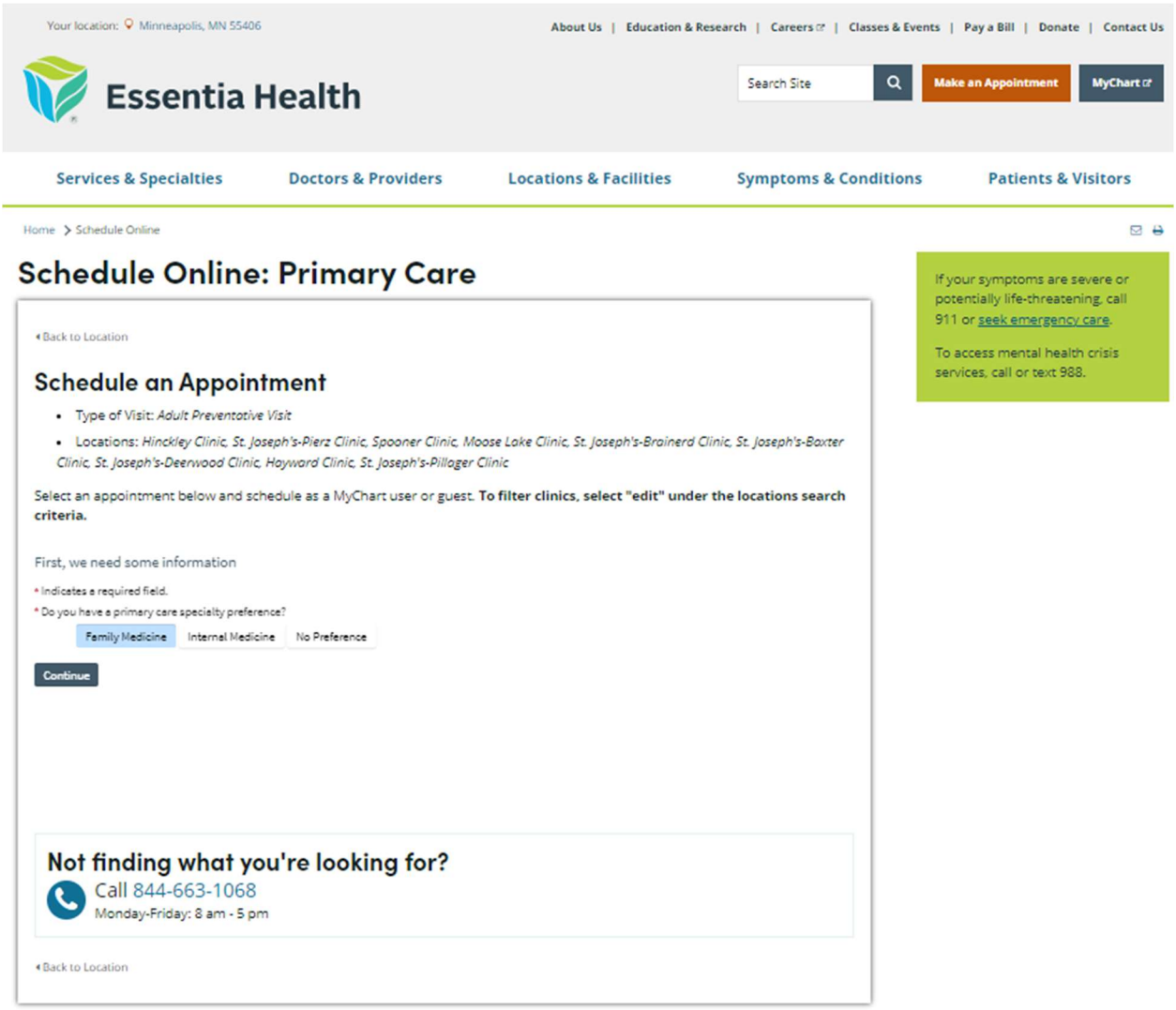
j. **Step 10:** Acknowledge that preventative care visits are covered by most insurance companies and recommended annually and select "Continue."



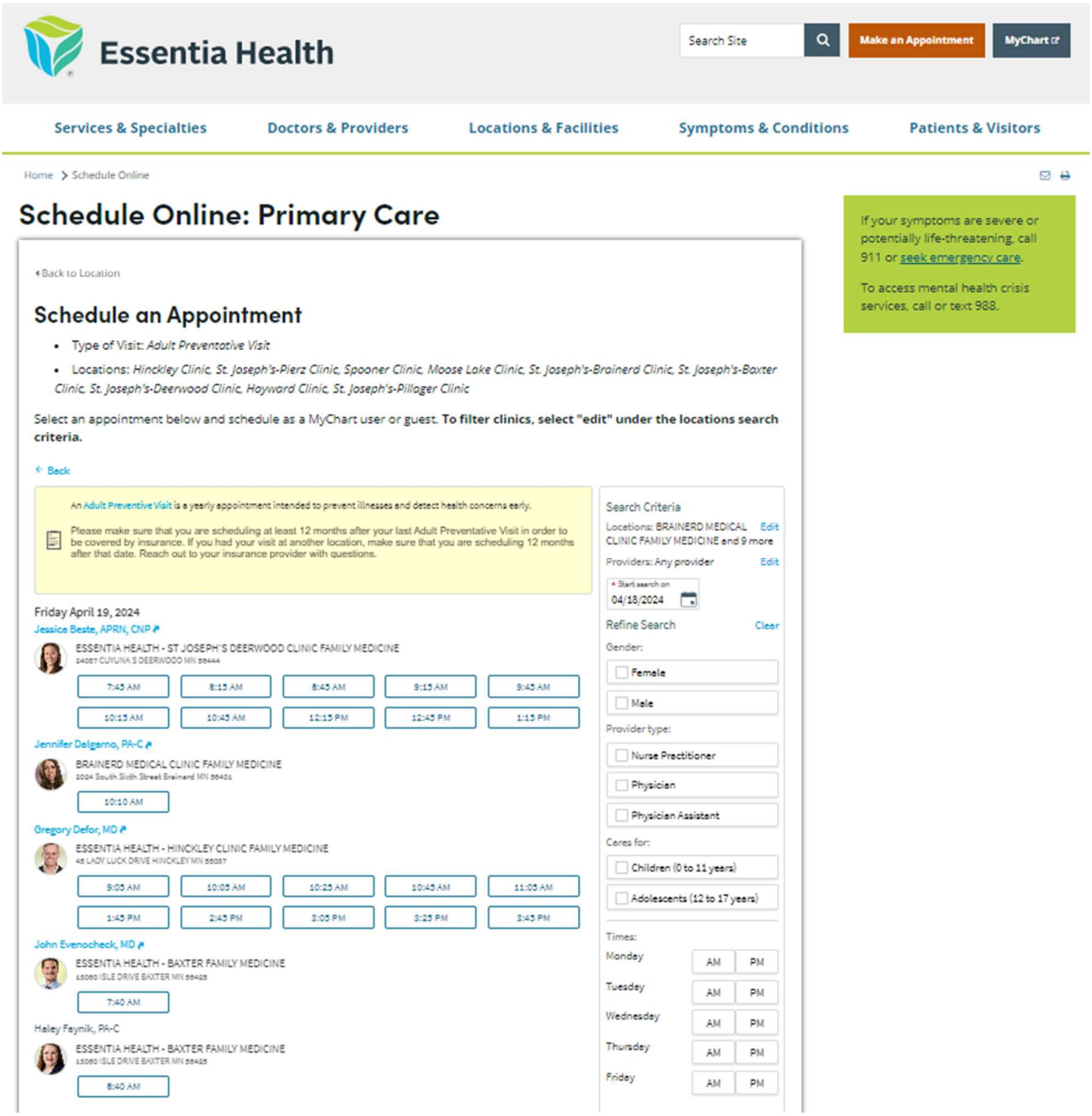
k. **Step 11:** Answer whether patient or prospective patient would like to establish a new primary care doctor with Essentia and select "Continue."



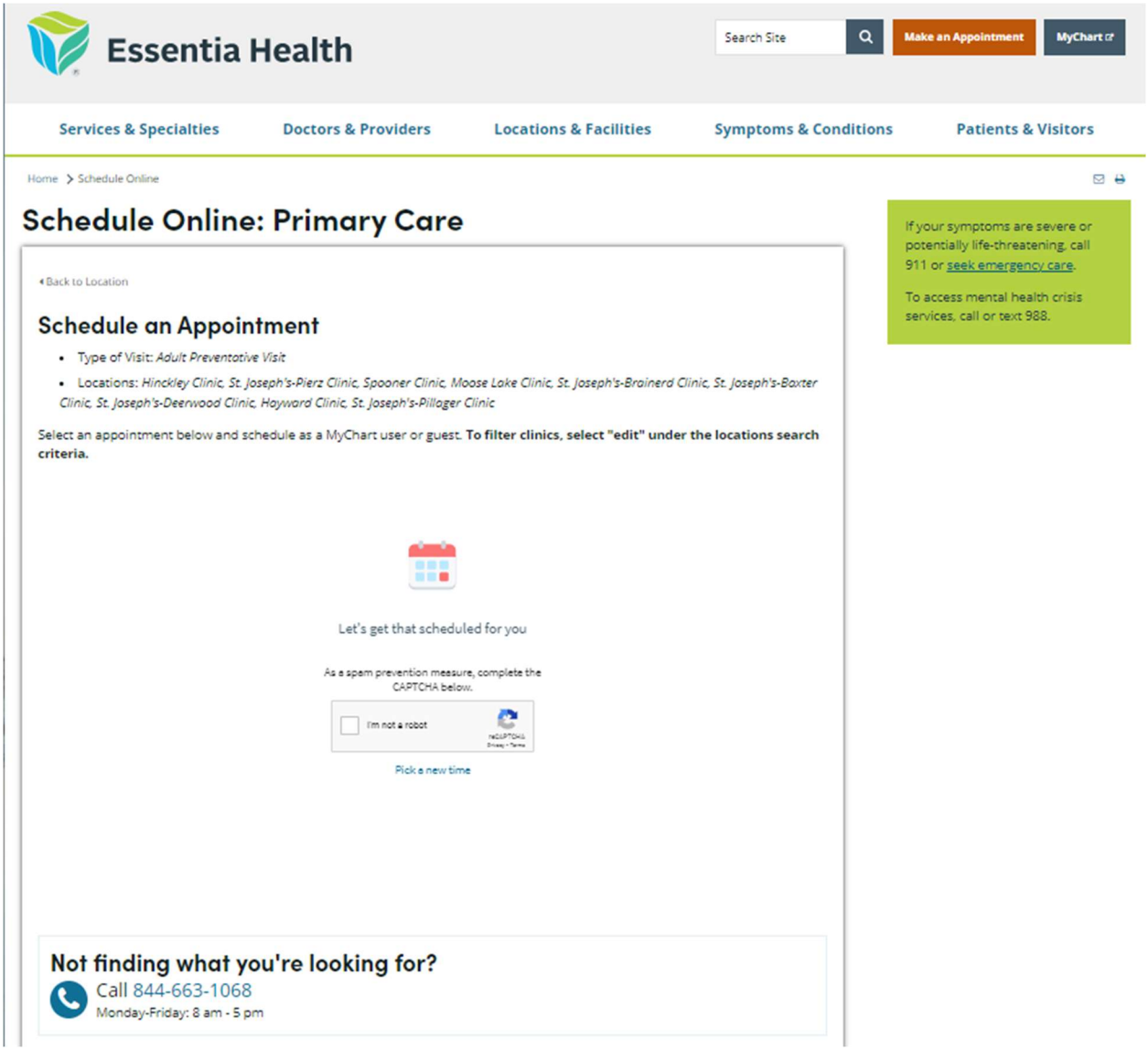
l. **Step 12:** Select a primary care specialty preference and select "Continue."



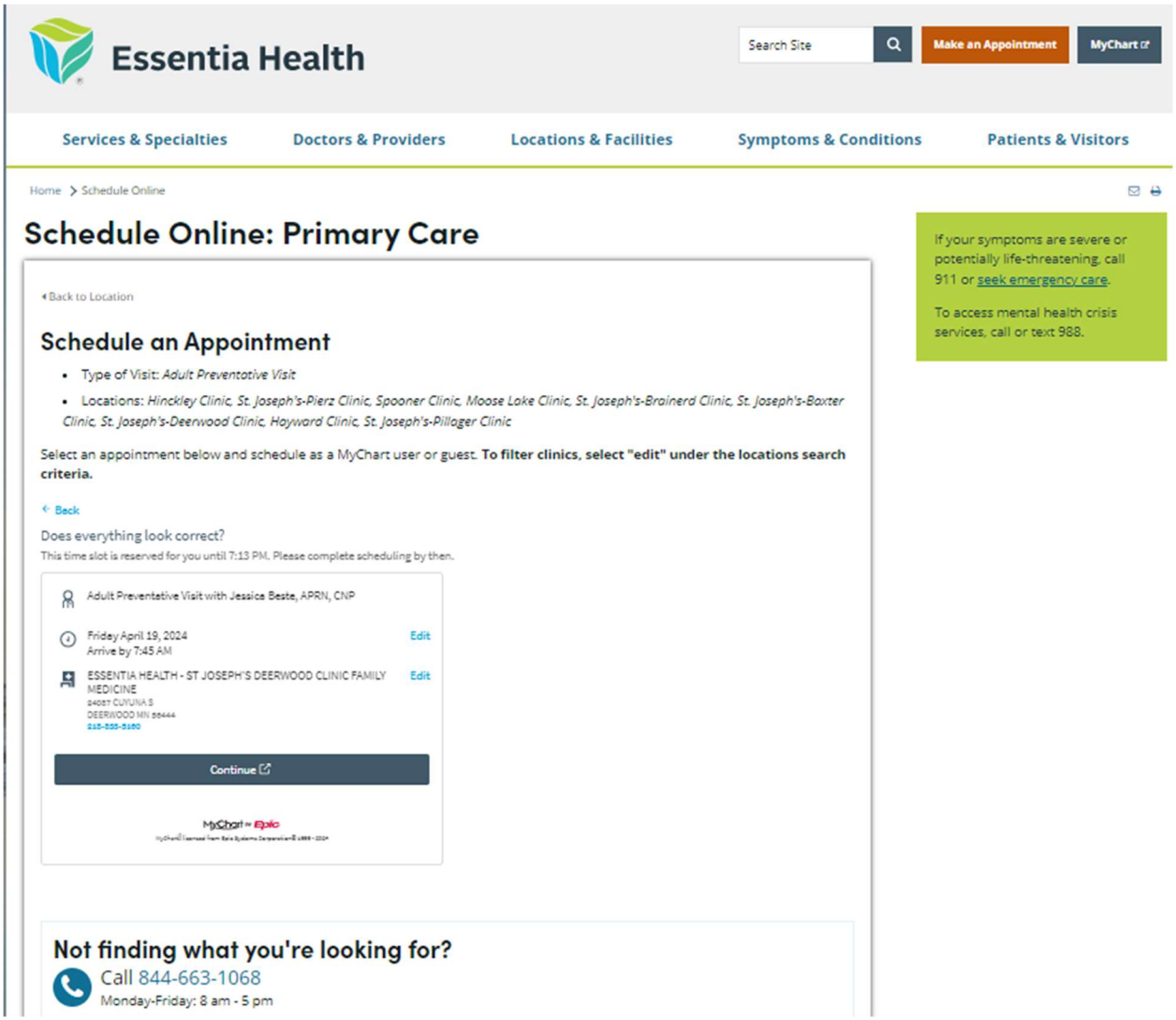
m. **Step 13:** Select an appointment from the listed options.



n. **Step 14:** Confirm that the patient or prospective patient is not a robot.

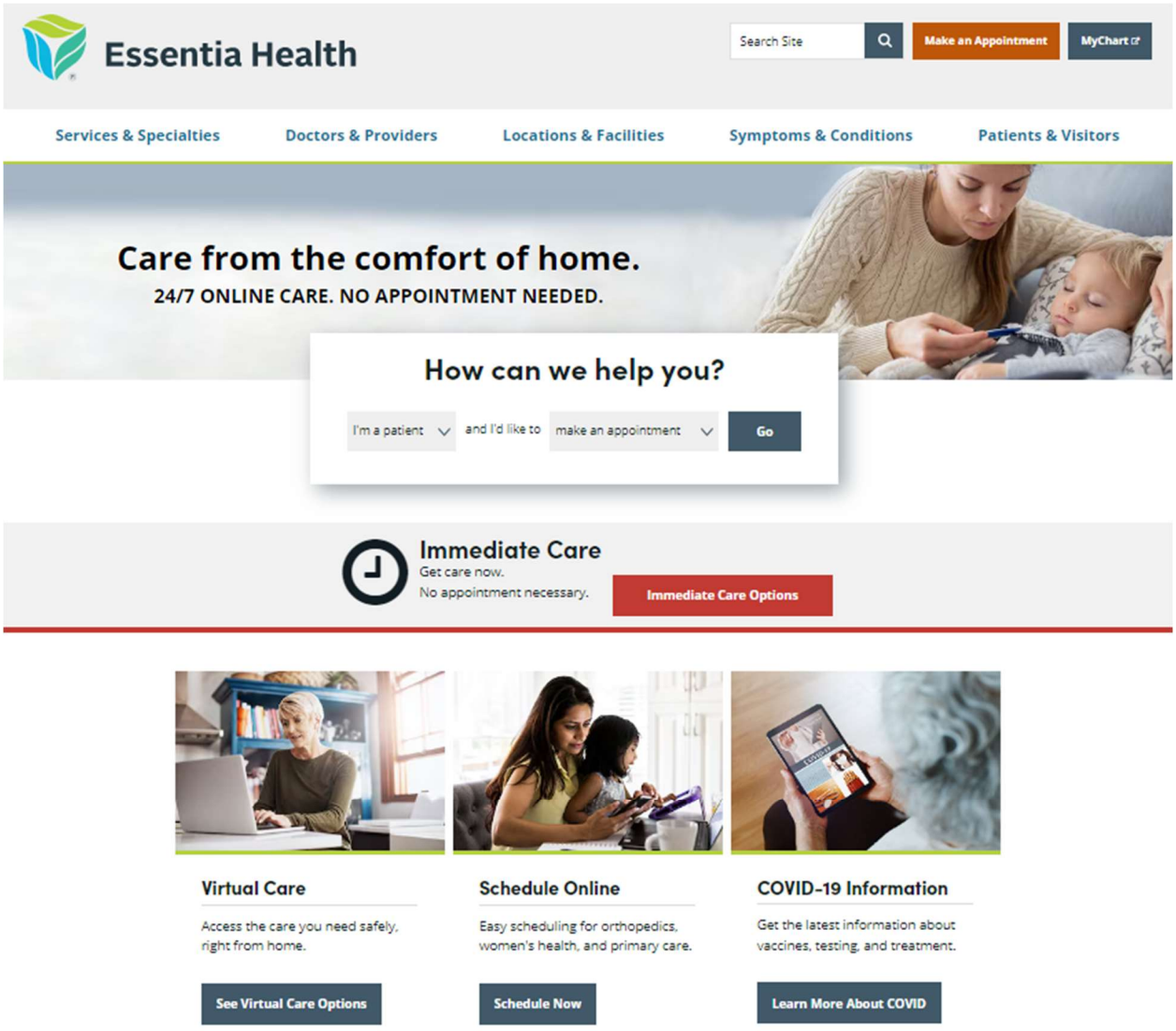


o. **Step 15:** Confirm the appointment choice by clicking "Continue."

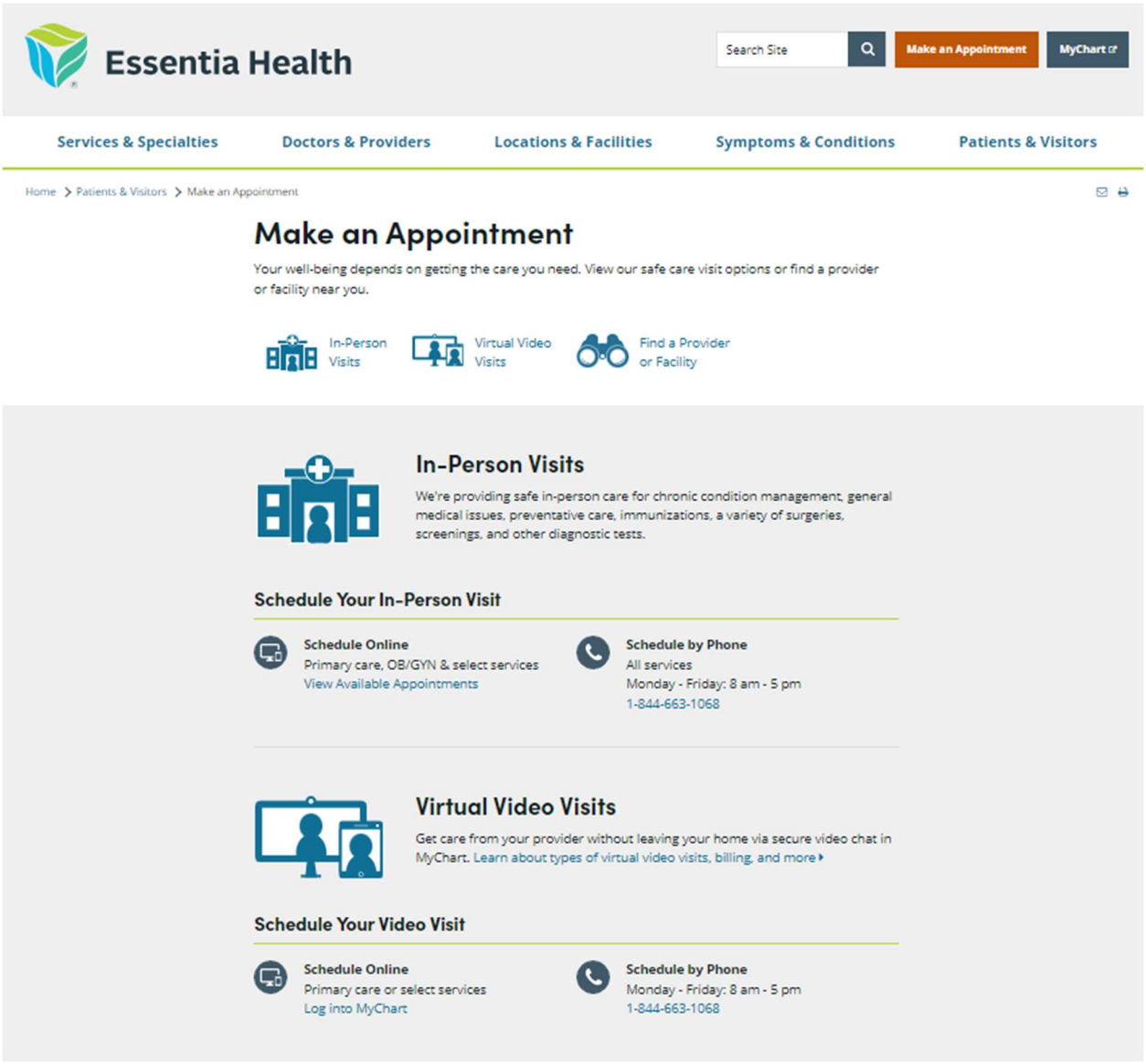


48. Below are several screenshots from Essentia's website demonstrating the types of information a 15 y/o female patient or prospective patient would submit to Essentia to make a first OBGYN appointment for pregnancy.

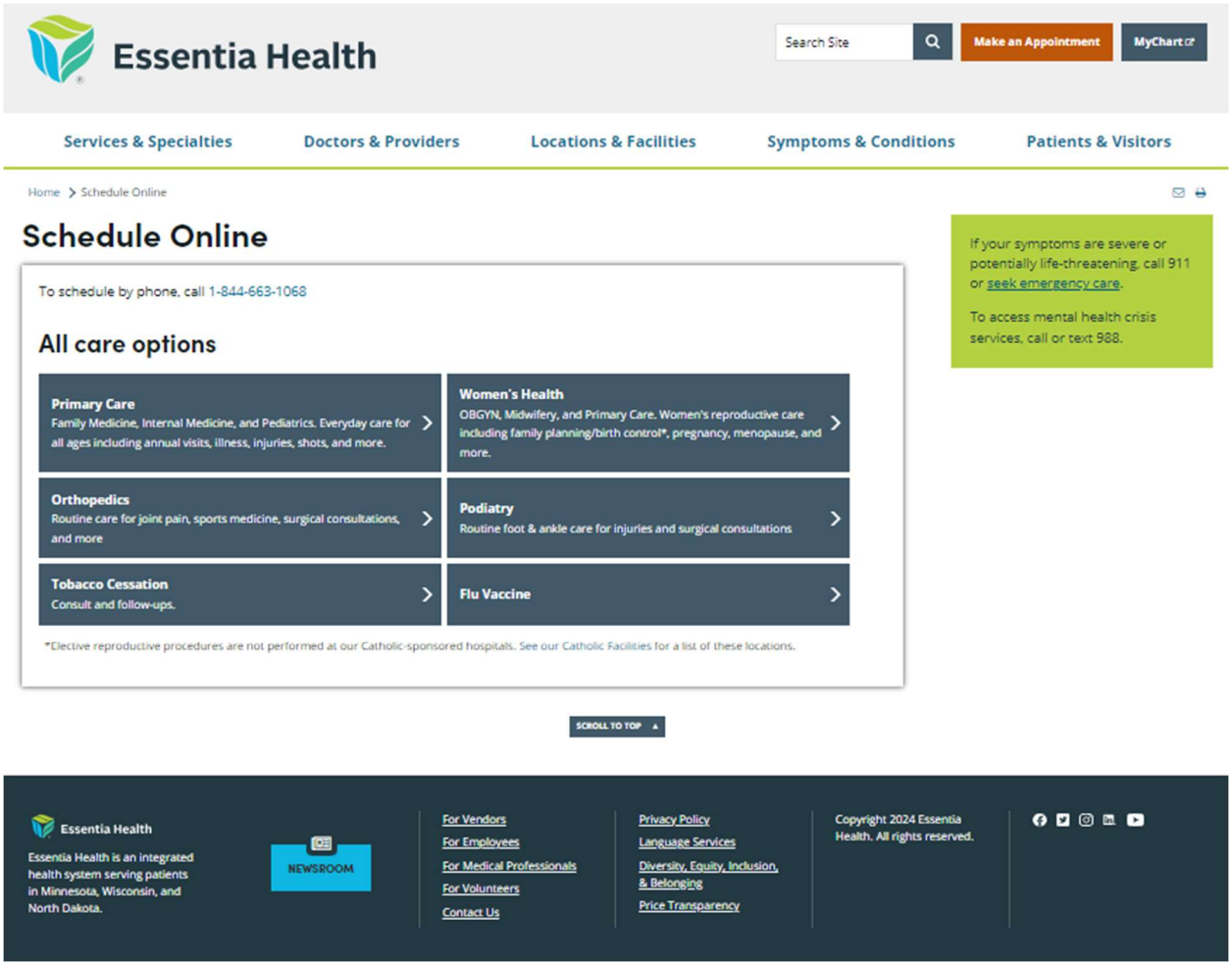
a. **Step 1:** Go to essentiahealth.org and select "I'm a patient" and I'd like to "make an appointment."



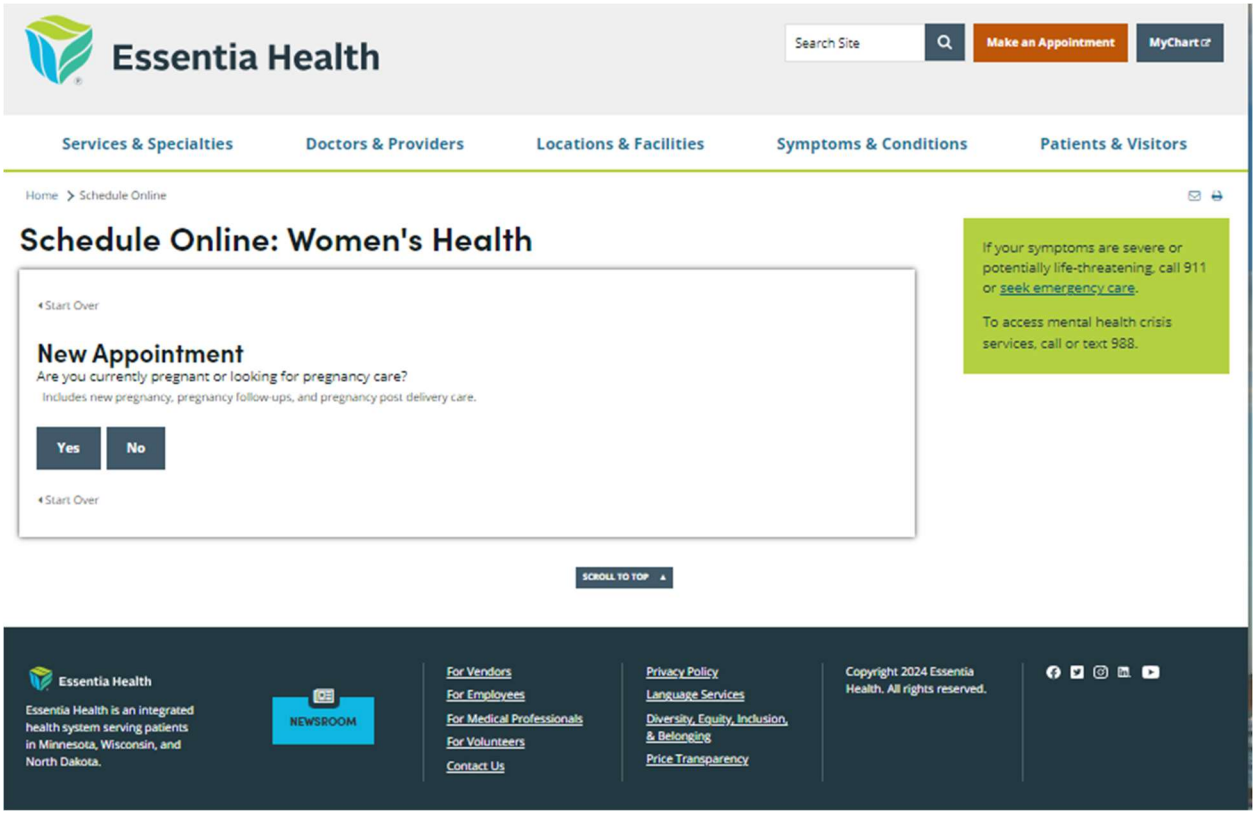
b. **Step 2:** Select "View Available Appointments" under the heading "Schedule Online."



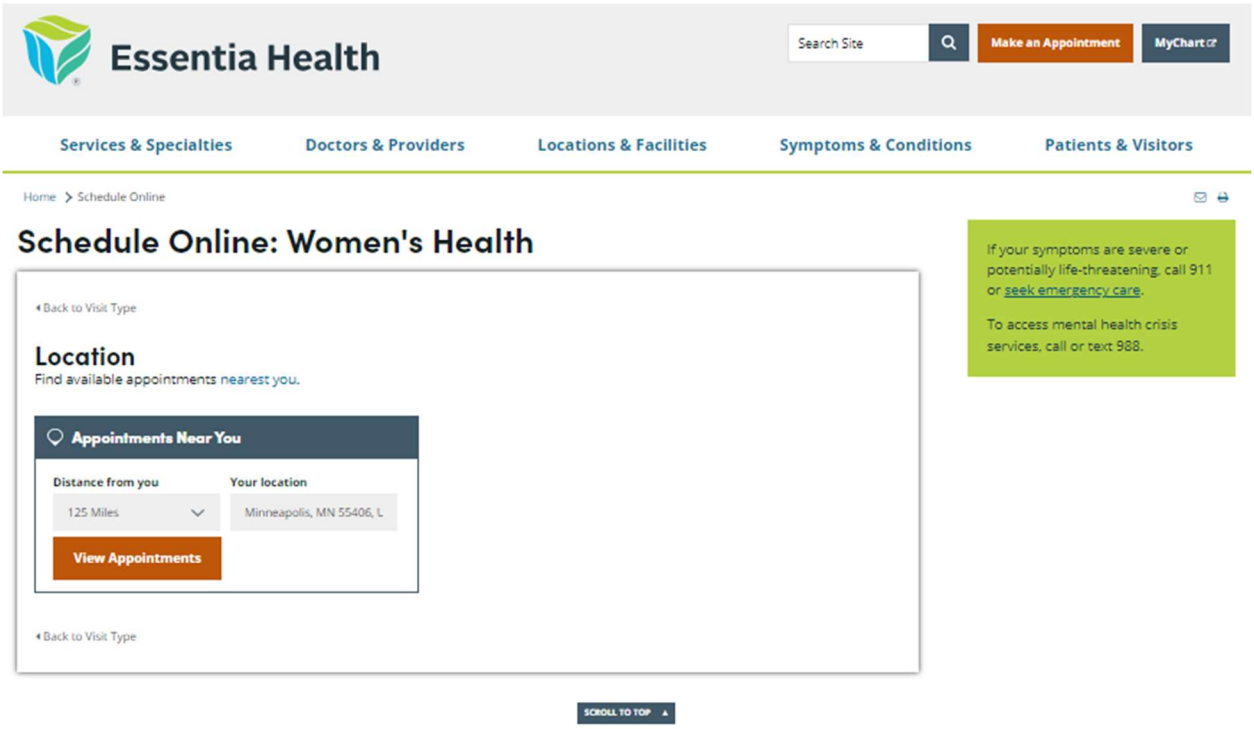
c. **Step 3:** Review "All Care Options" and select "Women's Health."



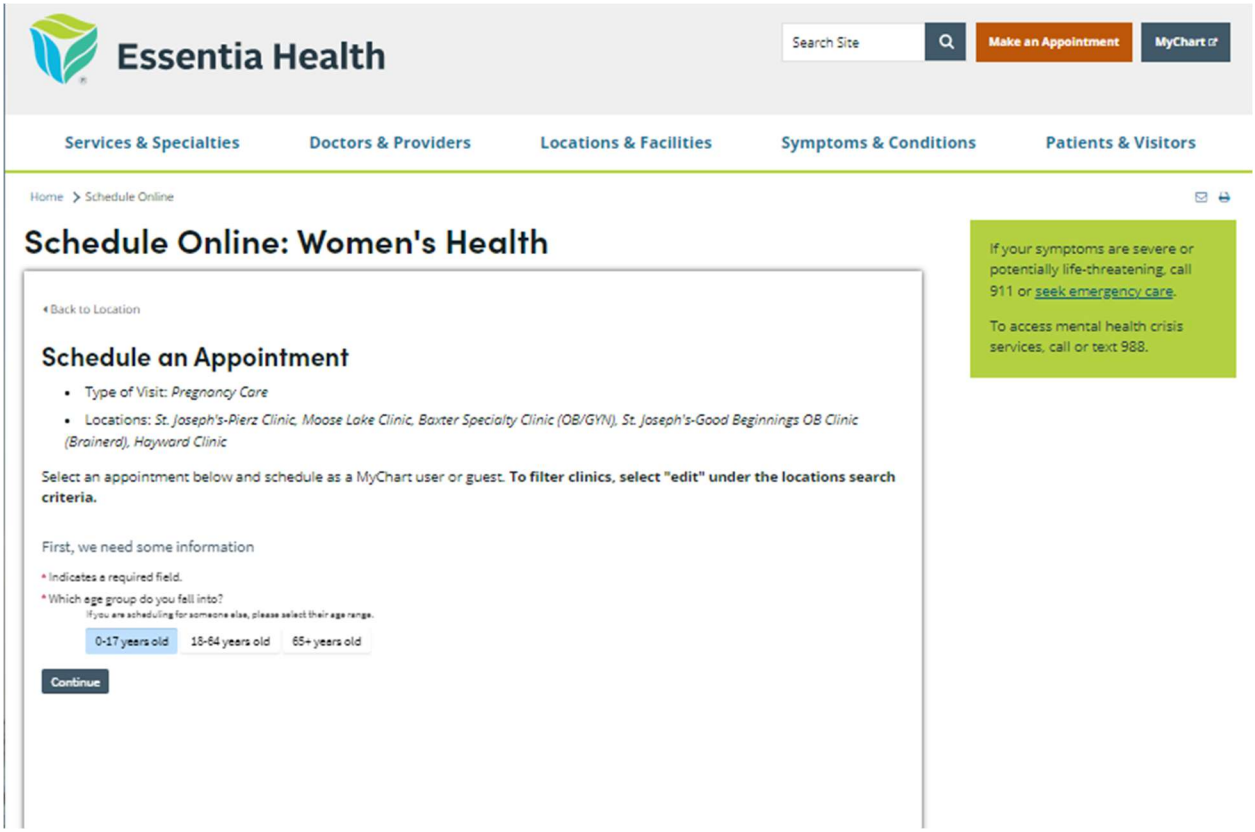
d. **Step 4:** Answer "Yes" to whether patient or prospective patient is currently pregnant or looking for pregnancy care."



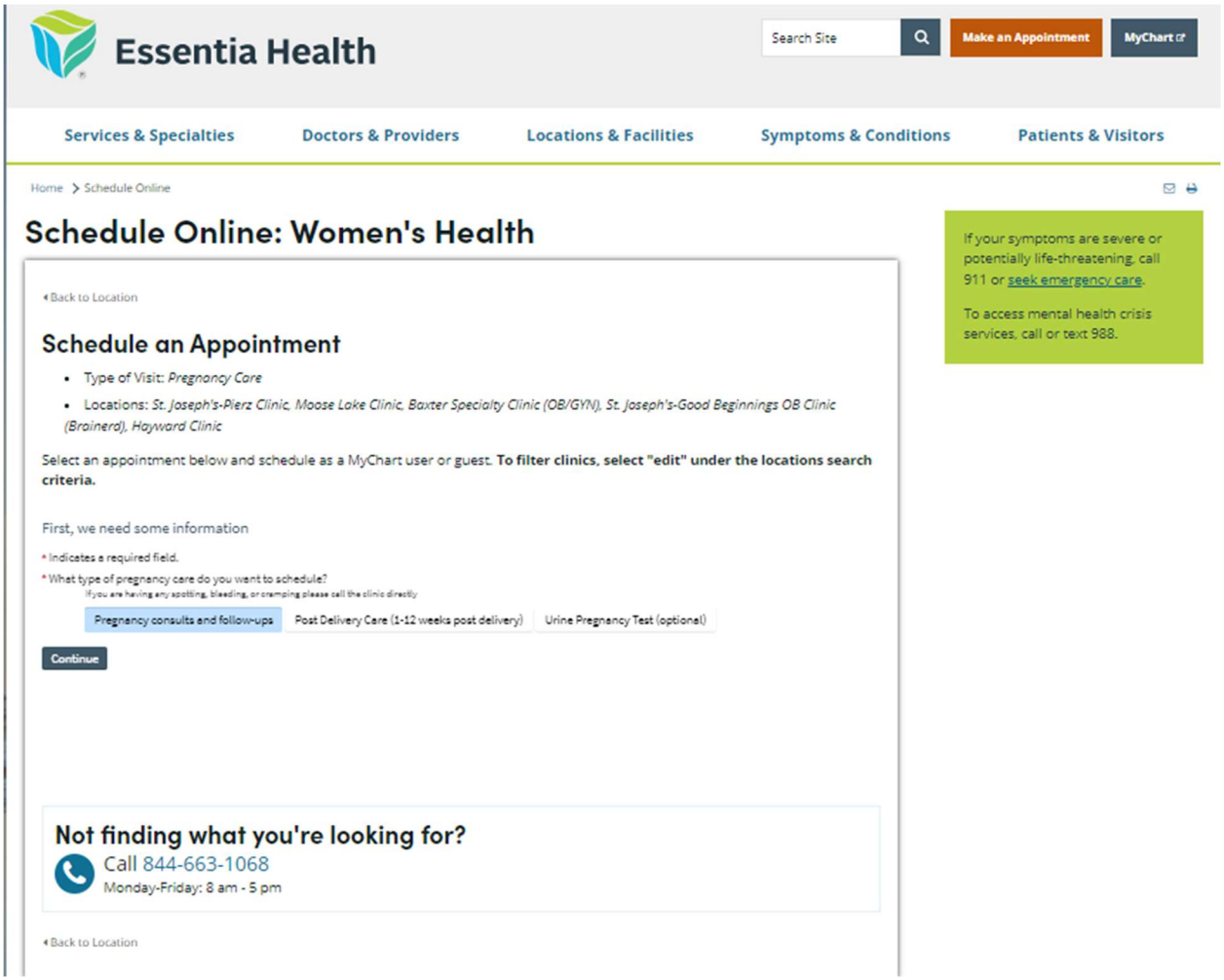
e. **Step 5:** Input location information to find an "Appointment Near You" and select "View Appointments."



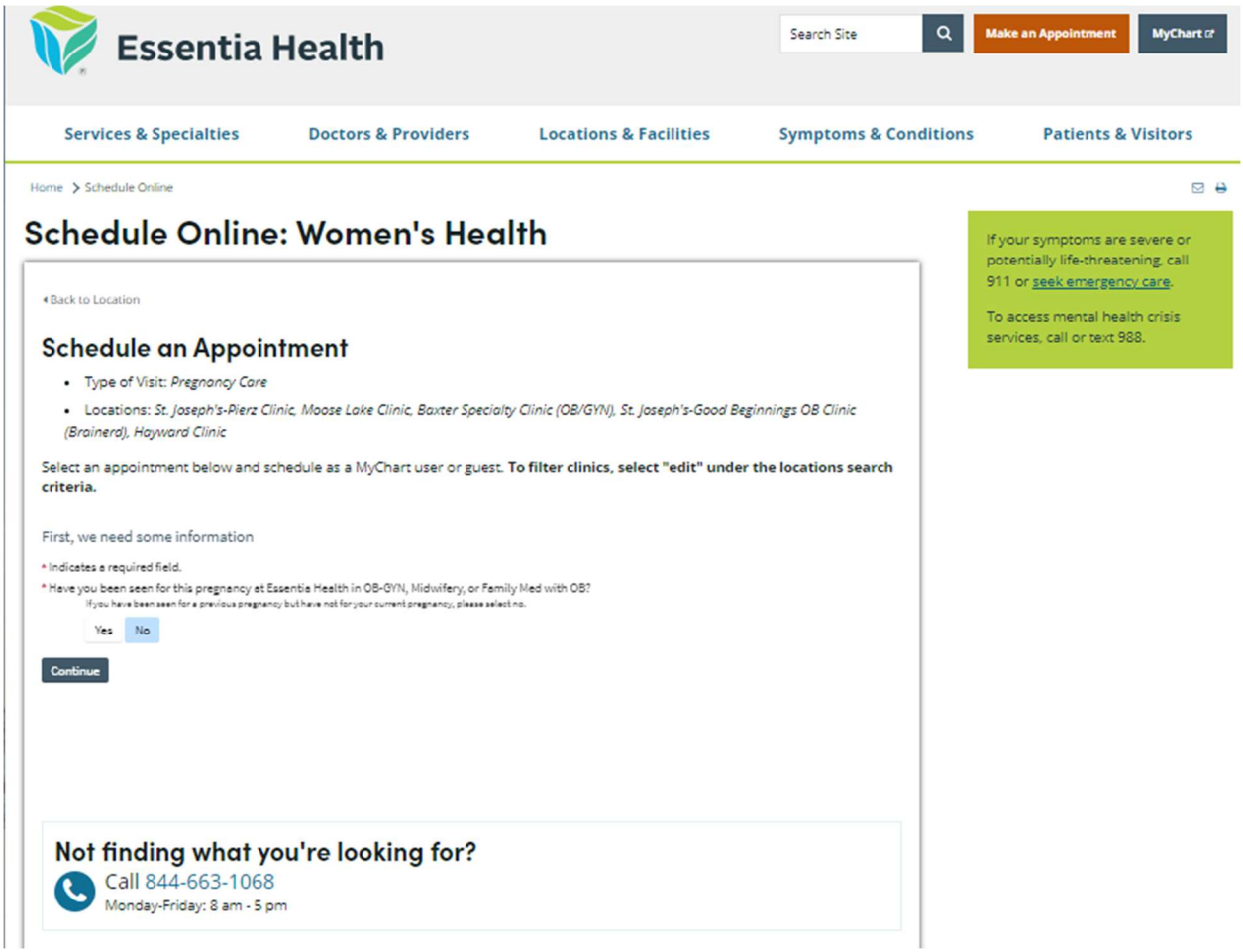
f. **Step 6:** Select "0-17 years old" from the age group options and select "Continue."



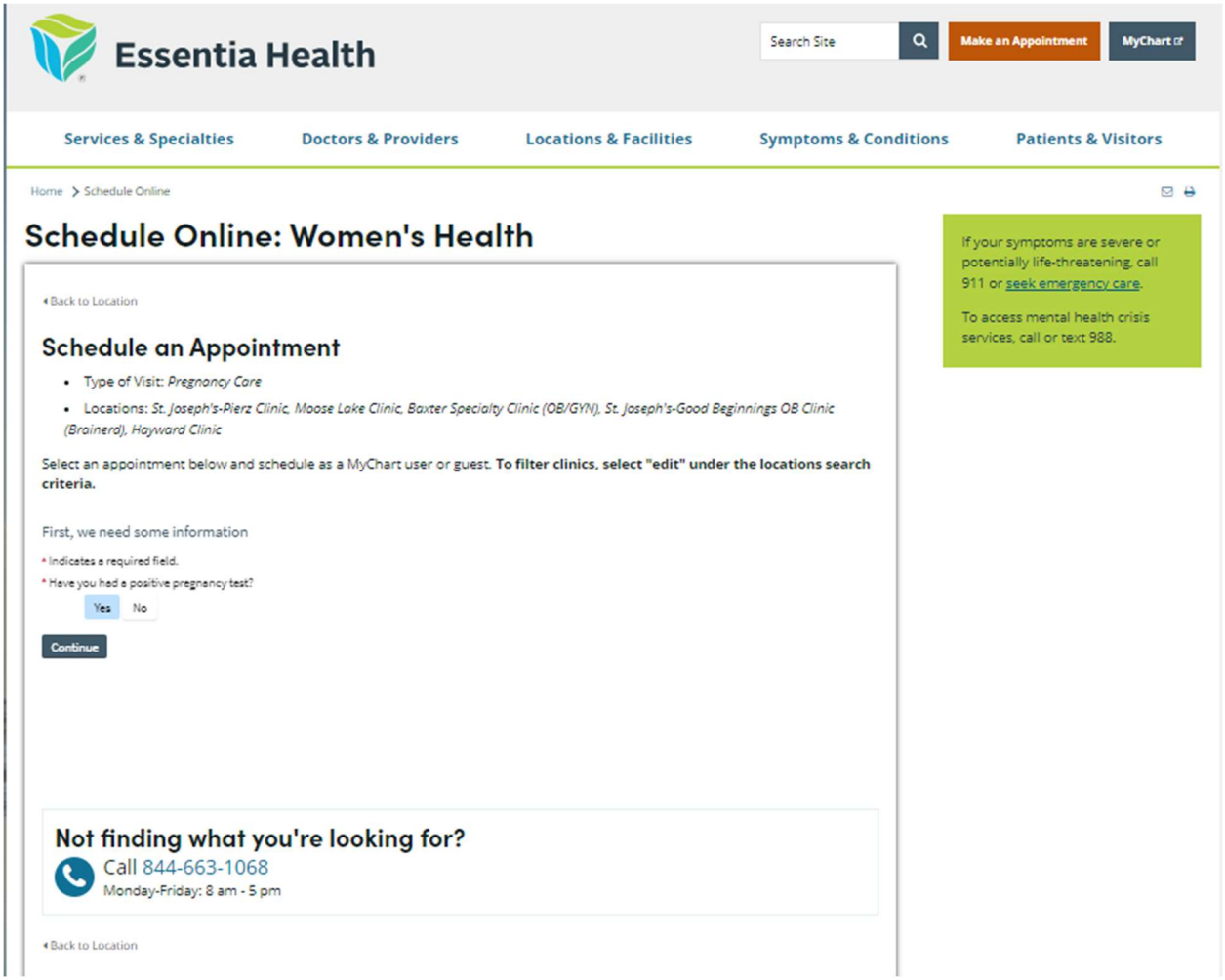
g. **Step 7:** Select from type of pregnancy care options "Pregnancy consults and follow-ups" and select "Continue."



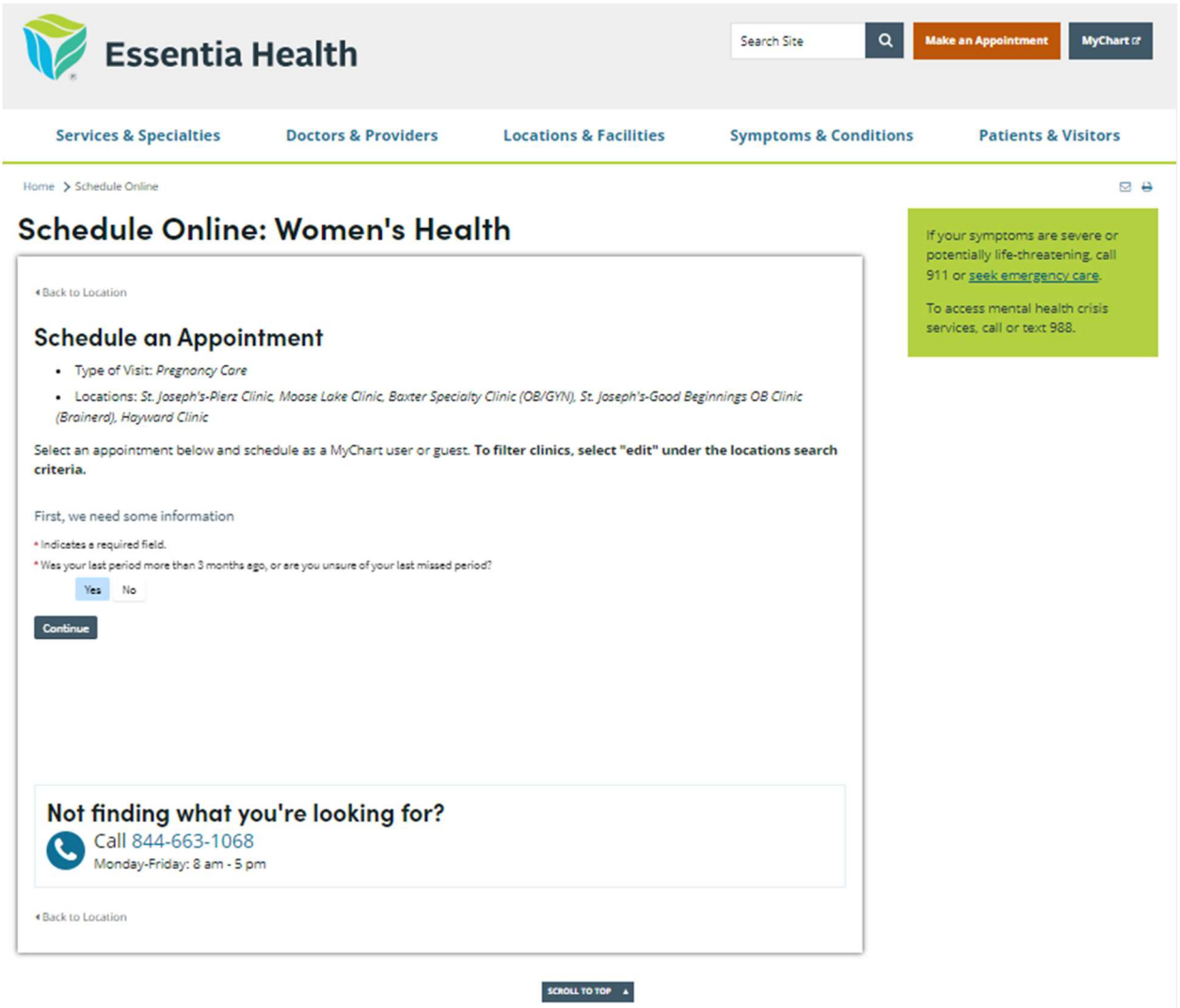
h. **Step 8:** Select "No" from prompt asking whether patient or prospective patient has been seen for this pregnancy at Essentia Health in OB-GYN, Midwifery, or Family Med with OB and select "Continue."



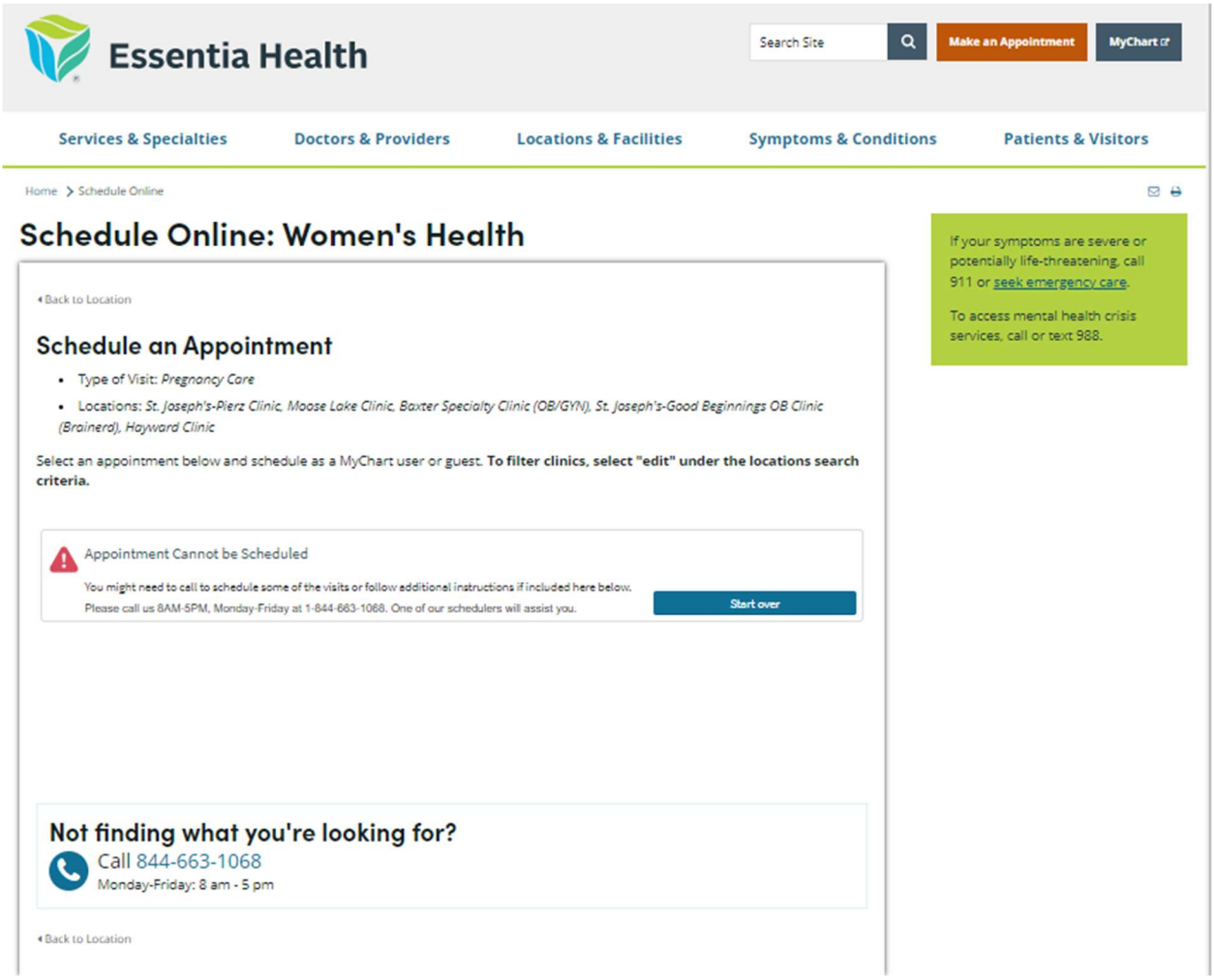
i. **Step 9:** Select "Yes" when as whether patient or prospective patient has had a positive pregnancy test and select "Continue."



j. **Step 10:** Confirm patient's or prospective patient's last period was more than 3 months ago, or that patient or prospective patient is unsure of last period and select "Continue."

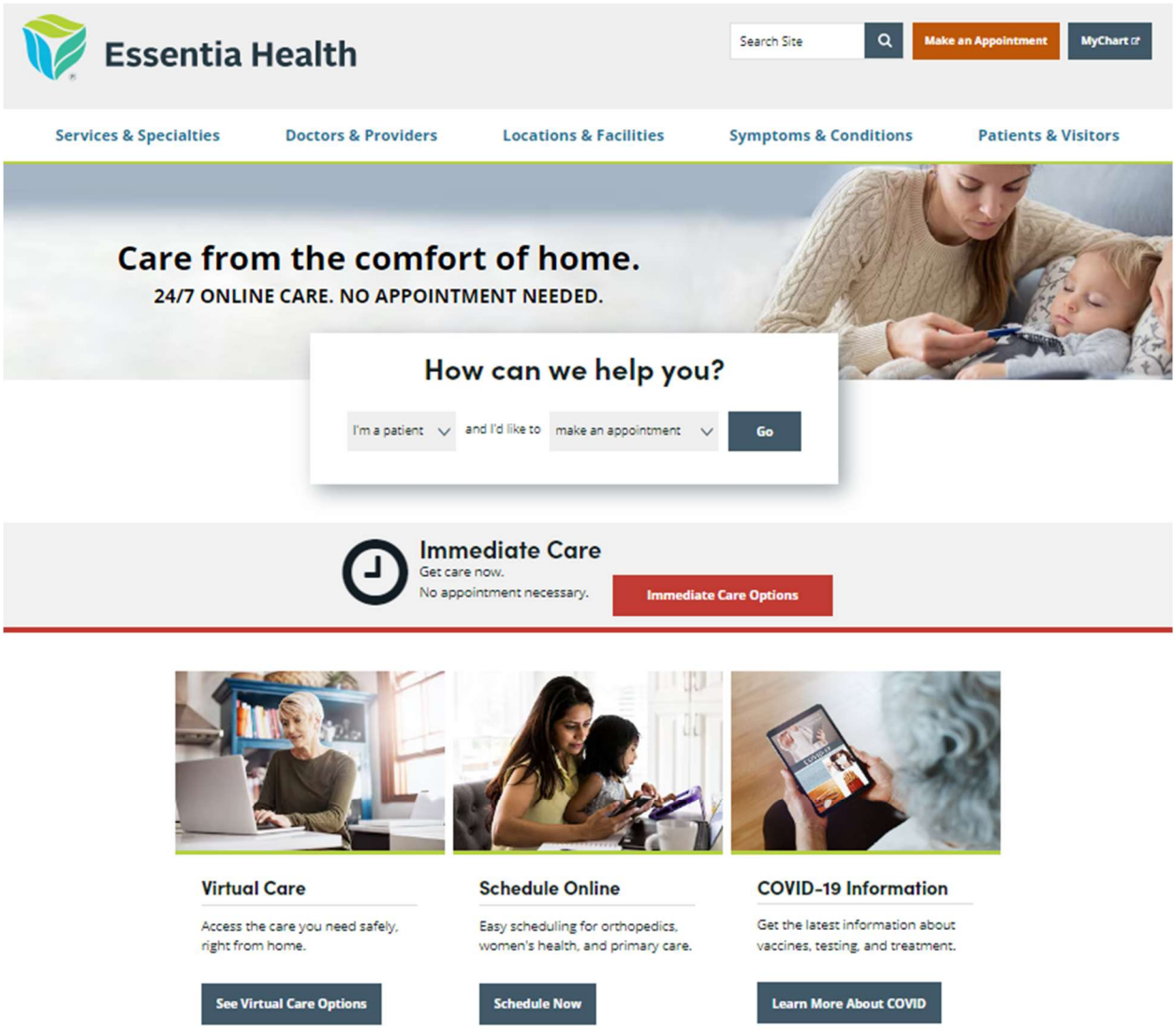


k. **Step 11:** After entering all of this personal information, the patient or prospective patient is directed to call to schedule.

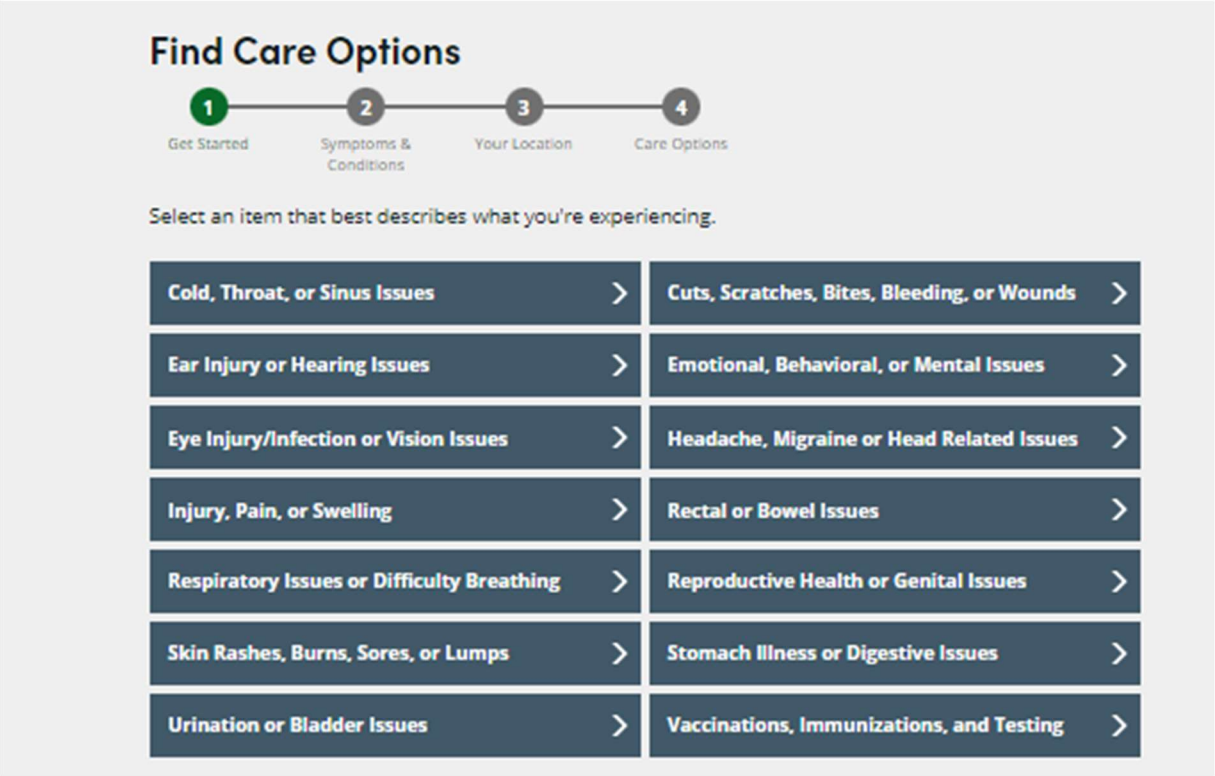


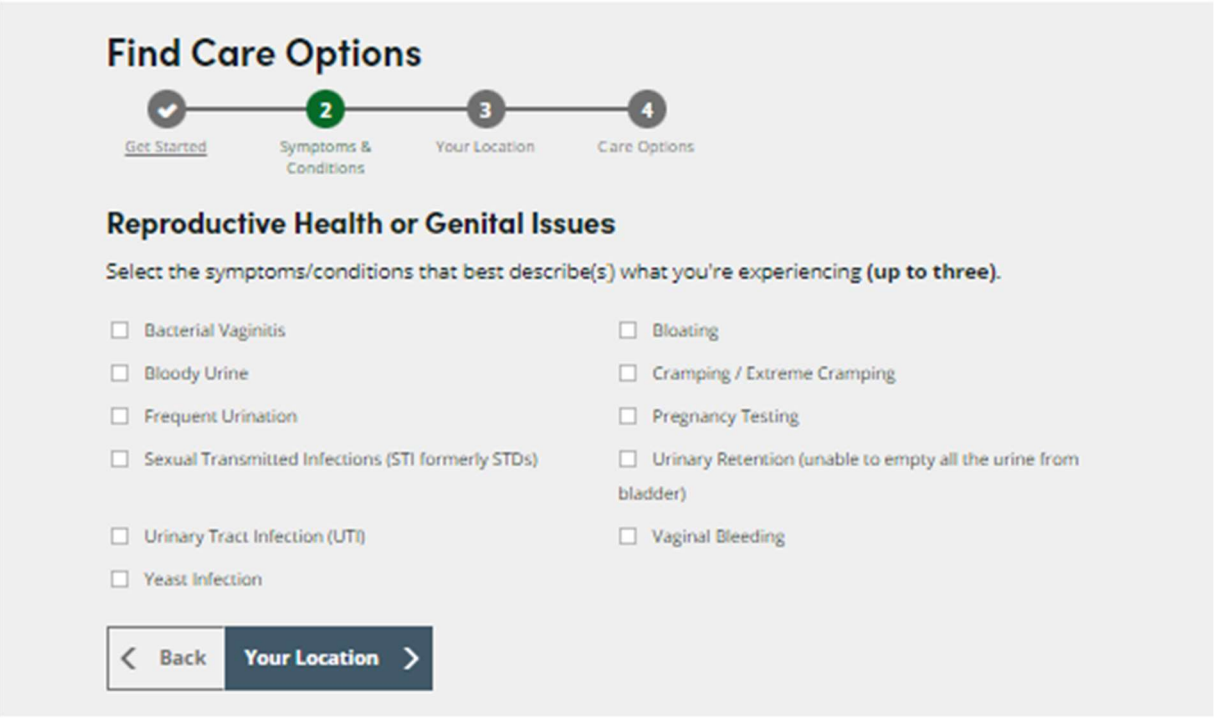
49. Below are several screenshots demonstrating the types of information an individual seeking immediate care from Essentia submits on the public facing website.

a. **Step 1:** Go to essentiahealth.org and select "Immediate Care Options."

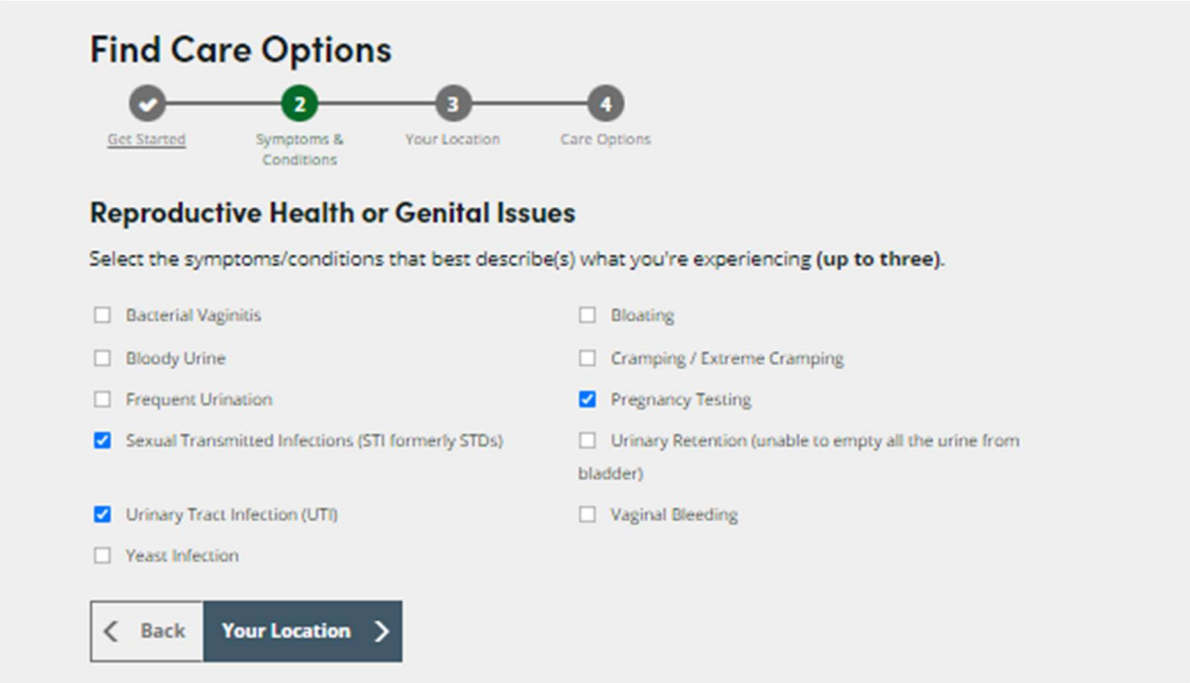


b. **Step 2:** Select an "Item that best describes what you are experiencing." For this example, the patient or prospective patient selected "Reproductive Health or Genital Issues."

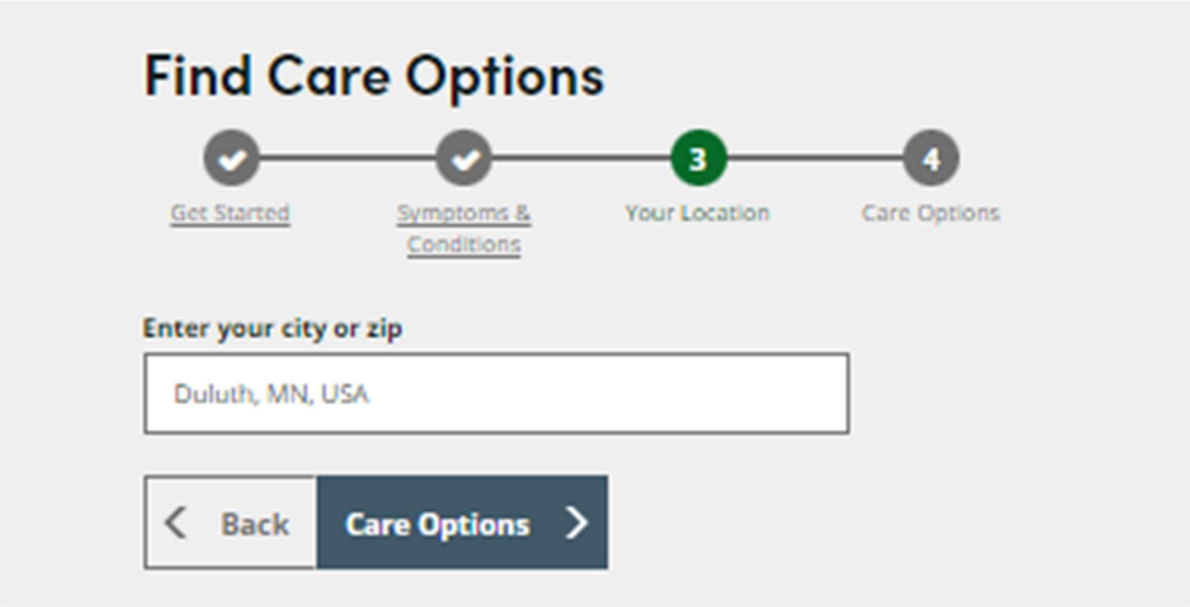




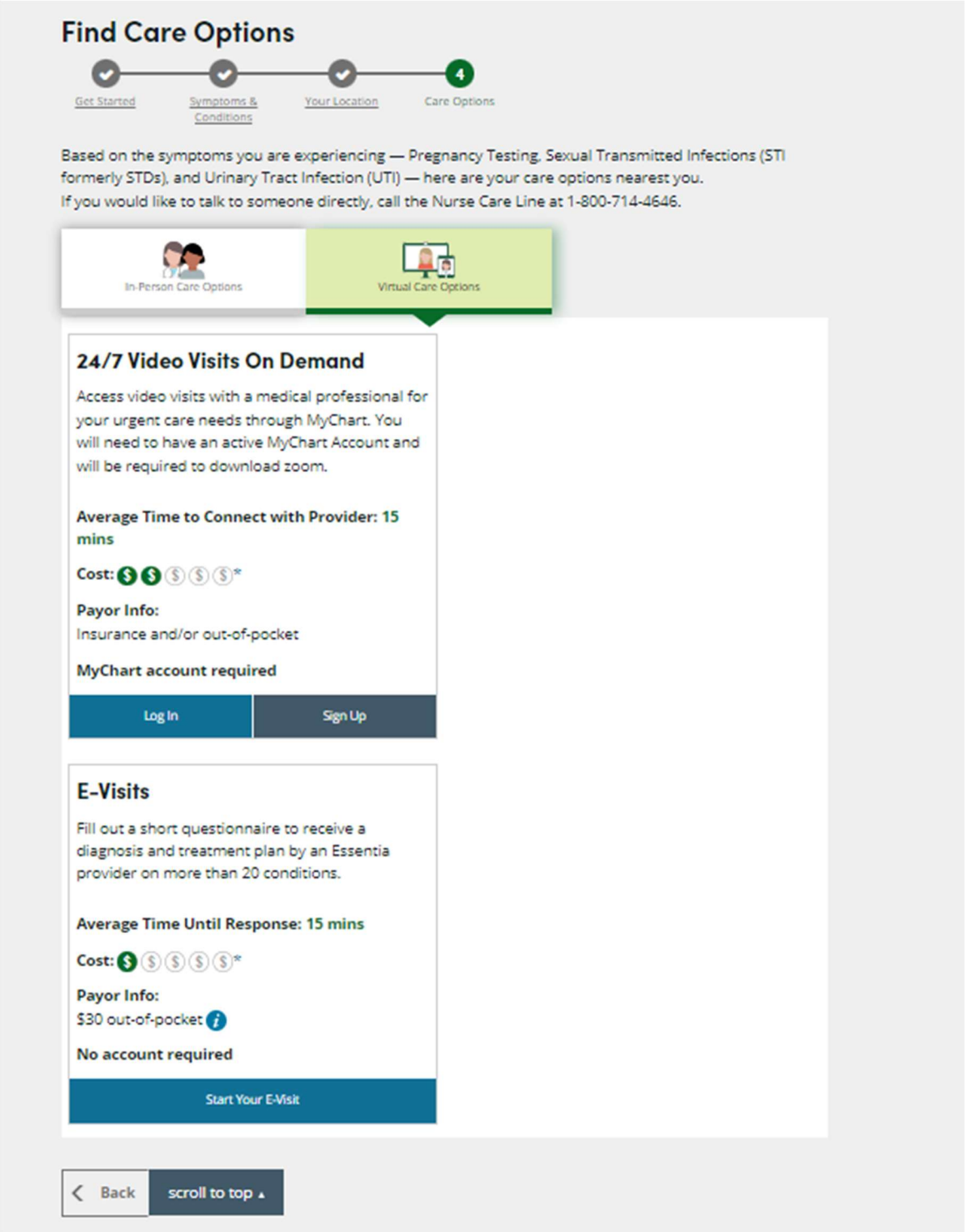
c. **Step 3**: Select the "symptoms/conditions that best describe(s) what you're experiencing (up to three)." For this example, the patient or prospective patient selected "Sexual Transmitted Infections (STI formerly STDs)," "Urinary Tract Infection (UTI)," and "Pregnancy Testing."



d. **Step 4**: Enter location information.



e. **Step 5:** Review "In-person" and "Virtual" care options. For this example, the patient or prospective patient selected "Start your E-Visit."



50. Patients and prospective patients communicate all of the above information on Essentia's website without ever logging into MyChart. When information, such as the sensitive, health information described above, is intercepted by the Meta Pixel, Meta receives it in a manner by which Meta can identify the individual, either by Facebook account number or some other identifier.

51. Defendant tells patients it will keep their Sensitive Information secure and private. Indeed, Defendant represented that it is committed to doing what's right by following the highest business ethical standards. It stated that it will comply with all applicable laws and regulations as well as its own internal policies and procedures.[26]

52. Essentia maintains a "Health Code of Integrity" in which it commits to "avoiding injuries to patients from the care that is intended to help them," "doing the right thing," "complying with laws, regulations, and applicable Essentia Health policies and procedures," "comply[ing] with various federal, state, and local laws and regulations that are in place to safeguard our patients and our organization," and "to provide the quality care reflected in recognized professional standards."[27]

53. Essentia also maintains a Privacy Policy through which it states, "Essentia Health is committed to protecting the privacy of those who visit our website."[28]

---

[26] *Id*.
[27] Code of Integrity, https://www.essentiahealth.org/app/files/public/7e69cc11-a4d4-43c9-89f0- 905e8cf7d8dd/Code-of-Integrity.pdf (last visited April 15, 2024).
[28] Website Privacy Policy & Terms of Use (Patient), https://www.essentiahealth.org/about/privacy-legal-notices/website-policy/ (last visited April 15, 2024).

54. Plaintiff and the Class members had a reasonable expectation of privacy and relied on Defendant to protect the Sensitive Information provided to it and created by it, especially because medical facilities are always required to maintain confidentiality of patient records, with very limited exceptions. Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. Moreover, through its various policies, Defendant acknowledged its obligation to reasonably safeguard sensitive information against unauthorized disclosure of Sensitive Information to third- parties like Meta.

55. A privacy violation of this type, in which Defendant intentionally granted access to third-party Meta to record and collect user data on the company's website, including Sensitive Information and highly confidential medical records without restriction, could not occur but for Defendant's blatant disregard of users' privacy. Defendant violated basic privacy and data standards regarding patient privacy and confidentiality.

56. As described throughout this Complaint, Defendant did not reasonably protect, secure, or store Plaintiff and the Class member's Sensitive Information but rather intentionally and knowingly granted Meta access to confidential information that it knew or should have known was unlawful.

57. Consequently, Meta, and potentially other third parties, obtained access to and collected confidential patient data without the patients' authorization, resulting in a significant invasion of patient privacy and breach of sensitive data.

B. Defendant Exposed Its Patients' Sensitive Information

58. Defendant implements Meta's Pixel on its website and applications. Pixel tracks website and application users' activity. If a user accesses a website hosting Pixel, Meta's software will secretly direct the user's browser to send a separate message to Meta's servers. This second communication contains the original request the user sent to the host website, in this case Defendant's, along with the additional data Pixel is configured to collect. This communication happens concurrently with the first communication the user initiates with the host website.

59. To illustrate this process, consider a patient who opens Defendant's website and clicks on the "Doctors & Providers" tab. When the user clicks this tab, his browser sends a request to Defendant's server requesting that server load the "Doctors & Providers" page. Because Defendant utilizes Meta's Pixel, Meta's code surreptitiously duplicates the communication from the user to Defendant and sends it to Meta's own servers, along with additional information that includes the user's identity via a Facebook account number or other identifying information.

60. After collecting this information, Meta can process it and add it to their aggregates of consumer data, which may ultimately be used for advertising or other revenue generating schemes, including ads posted on Essentia's webpage.

61. Every time Defendant sends patients' data to Meta, the patients' Sensitive Information is unlawfully disclosed. Defendant could have configured its website and applications to not communicate or share any information with third parties, or to limit the information it communicated to third parties, and maintain the necessary security and

confidentiality, but it did not.

62. Upon information and belief, Defendant intercepted and disclosed the following non-public private information to Meta: (1) Plaintiff's and the Class members' status as medical patients, or alternatively, Plaintiff and the Class members' consideration of becoming a medical patient of Defendant; (2) Plaintiff's and the Class members' communications with Defendant; (3) Plaintiff's and the Class members' medical appointments, location of treatments, specific medical providers, and specific medical conditions and treatments; (4) PII including but not limited to patients' locations, an IP address, device identifier, and/or an individual's unique Facebook user number ("FID").

63. Despite the highly sensitive nature of the information Defendant obtained, created, and stored, Defendant inexplicably failed to take appropriate steps to protect the privacy of the PII and PHI of Plaintiff and the Class, and instead intentionally employed Pixel to willingly disclose patient data to third-parties including Meta.

64. Defendant deprived Plaintiff and the Class members of their privacy rights when it: (a) implemented Pixel that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications and private information; (b) disclosed patients' protected information to Meta—an unauthorized third-party; and (c) failed to provide notice to Plaintiff and the Class members or obtain their consent to share their Sensitive Information with others.

C. The Meta Pixel

65. Meta's core business function is to sell advertising and it does so on several platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in

annual revenue comes from advertising—a practice in which Meta actively participates in using algorithms that approve and deny ads based on the ads' content, human moderators that further review ads, for both legality and aesthetics prior to and after publishing the ads, and other algorithms that connect ads to specific users, without the assistance or input of the advertiser.

66. Over the last decade Meta has become one of the largest and fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily, monthly, and annual user base has grown exponentially to billions of users.

67. Meta's advertising business has been successful, due, in significant part, to Meta's ability to target its users, both based on information users provide to Meta, and other information about users Meta extracts from the internet at large. Given the highly specific data used to target specific users, thousands of companies and individuals utilize Facebook's advertising services.

68. One of Meta's most powerful advertising tools is the Meta Pixel, which Facebook first launched in 2015.

69. Meta branded Pixel as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website." Meta further stated:

> Facebook pixel, [is] a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website. We're also announcing the availability of custom conversions, a new rule-based method to track and report conversions for your Facebook ads.
>
> Facebook pixel makes things simple for advertisers by combining the functionality of the Conversion Tracking pixels and Custom Audience pixels into a single pixel. You only need to place a single pixel across your entire website to report and optimize for conversions. Since it is built on top of the upgraded Custom Audience pixel, all the features announced in our previous

> blog post (Announcing Upgrades to Conversion Tracking and Optimization at Facebook) are supported through Facebook pixel as well.
>
> [Advertisers and website operators] can use Facebook pixel to track and optimize for conversions by adding standard events (e.g., Purchase) to your Facebook pixel base code on appropriate pages (e.g. purchase confirmation page).[29]

70. Websites are hosted by computer servers, through which the entity in charge of the website exchanges communications with Internet users via their web browsers. The set of instructions that command the browser is called the source code. The source code can command a web browser to send data transmissions to third parties via pixels, which can allow a website to export data about users and their actions to third parties. The third parties receiving this data are typically configured to track user data and communications for marketing purposes.

71. The pixels are invisible to the website users and thus, without any knowledge, authorization or action by the user, the website site developer (website commander) can use its source code to contemporaneously and invisibly re-direct the user's PII and other non-public medical information to third parties.

72. Meta offers Pixel as a piece of code to integrate into websites, like Defendant's Website as among other things, a tool to help increase profits and revenue. As the name implies, Pixel "tracks the people and the type of actions they take."[30] According to Meta, Meta's Pixel is a piece of code that allows Defendant to "understand the

[29] Cecile Ho, Announcing Facebook Pixel, Meta (Oct. 14, 2015) https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/.

[30] Facebook, Retargeting, https://www.facebook.com/business/goals/retargeting (last visited April 15, 2024).

effectiveness of [its] advertising and the actions [prospective patients] take on [its] site."[31]

73. Through this technology, Meta intercepts each page a user visits, what buttons they click, as well as specific information they input into the website and what they searched. Pixel sends each of these pieces of information to Meta with PII, such as the user's IP address. Meta stores this data on its own servers, in some instances for years on end.

74. This data is often associated with the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits Defendant's website, Meta receives third party cookies allowing Meta to link the data collected by Meta Pixel to the specific Facebook user.

75. Meta can also link the data to a specific user through the "Facebook Cookie." The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users, including Facebook users. Additionally, Meta can link User Data to individual users by identifying information collected through Meta Pixel through what Meta calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching. Using Manual Advanced Matching the website developer manually sends data to Meta to link users. Using Automatic Advanced Matching, the Meta Pixel scours the data it receives to search for recognizable

[31] About Meta Pixel, https://www.facebook.com/business/help/742478679120153?id=1205376682832142 (last visited April 15, 2024).

fields, including name and email address to match users to their Facebook accounts.[32]

76. Pixel also allows Defendant to impact the delivery of ads, measure cross-device conversions, create custom audiences, learn about its website, and save money on advertising and marketing costs.[33] But, most relevant here, Pixel allowed Defendant and Meta to secretly track website users on Defendant's website and intercept their communications with Defendant. Indeed, Pixel is a bit of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

77. As an example of this, consider again, an individual who navigates to Defendant's website and selects the tab for "Doctors & Providers." When that tab is clicked, the individual's browser sends a GET request to Defendant's server requesting that server to load the webpage. Because Defendant employs Pixel on its website, Meta's embedded code, written in JavaScript, sends secret instructions back to the individual's browser, without alerting the individual it is happening.

78. Then, Meta causes the browser to secretly duplicate the prospective patient 's communication with Defendant, transmitting it to Meta's servers, alongside additional information that transcribes the communications' content and the individual's identity.

[32] Meta uses the hashed format specifically to link Meta Pixel data to Facebook profiles. *See* Anson Chan, Facebook Is Receiving Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022, 12:46 PM), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medicalinformation-from-hospital-websites.

[33] *Id.*

Thus, when Plaintiff and the Class members visited Defendant's website and entered their Sensitive Information, or inquired about sensitive personal things, that information was transmitted to Meta, including but not limited to details like the physician and appointment selected, treatments and care options, and specific button/menu selections. During that same transmission, Defendant would also provide Meta with the patient's Facebook ID number, IP address or device ID or other personally identifying information. This information makes it easy to identify the patients through the collection of identifying information that was improperly disclosed.

79. Once Meta has the data, it can process it, analyze it, and assimilate it into databases like Core Audiences or Customer Audiences for advertising purposes. If the patient or prospective patient is also a Facebook user, Meta will associate the information that it collects from the visitor with a Facebook ID that identifies their name and Facebook profile. In sum, Pixel allows Meta to learn, and use for its financial gain, the medical and private content Defendant's prospective patients viewed on Defendant's website. Essentia, similarly, benefits because refined ads using the ill-gotten information are then directed towards Plaintiffs and the Class. In short, Essentia and Meta gather Sensitive Information from Essentia's website users and, subsequently, use that private medical information to craft advertisements to their own benefit and in violation of state and federal law.

D. Defendant Employs Pixel on its Website to Allow Meta to Intercept Communications and Class Members' Sensitive Information.

80. By employing Pixel on its website, Defendant shares with Meta its patients' and prospective patients' identities, website activity, private communications, search requests and

results related to private medical treatment.

81. A single browsing session online may consist of thousands of website communications. Website communications include Requests (HTTP or HTTPS) and Responses (HTTP or HTTPS), and any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies.

82. An HTTP Request is an electronic communication a prospective patient sends from his device's browser to the website's server. There are two types of HTTP Requests: (1) GET Requests, which are one of the most common types of HTTP Requests. In addition to specifying a particular URL (i.e., web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies; and (2) POST Requests can send a large amount of data outside of the URL. In this case, a patient's HTTP Request would be asking Defendant's Website to get certain information, like a list of clinic locations or providers. and POST Requests, which can send a large amount of data to the host server embedded inside the URL and can include cookies.

83. Cookies are a text file that website operators and others use to store information on the visitor's device, and these can later be communicated to a server or servers. Cookies are sent with HTTP Requests from prospective patient's devices to the host server. Pixel uses both first- and third-party cookies. A first party cookie is created by the website the user is visiting, in this case Defendant.[34] Third party cookies are created by a website with a domain name other than the one the user is visiting, in this case

[34] *First-Party Cookie*, PCMAG.com, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is also confirmable using web developer tools to inspect a website's cookies and track network activity.

Facebook or Meta.[35] Meta uses both first- and third-party cookies to link Facebook IDs and Facebook profiles. Defendant sent these identifiers to Meta.

84. An HTTP Response is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the prospective patient's device's web browser from the host server. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data. Basically, the HTTP Response is when the website sends the requested information (see the HTTP Request) and is sometimes called the "Markup."

85. Websites, including Defendant's, also always include source code, which are the instructions and commands for the website that require the prospective patient's browser to take certain actions when the web page loads and when the user makes certain requests of the webpage. Source code, like Pixel, can also command a web browser to transmit data to third parties in the form of an HTTP Request. This is done without the knowledge of the prospective patient.

86. Defendant shares its patients' and prospective patients' identities and online activity, including private communications and search results related to private medical treatment.

[35] *Third-Party Cookie*, PCMAG.com, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable using web developer tools to inspect a website's cookies and track network activity. This is confirmable by tracking network activity.

87. Using the same example as before, when a patient or prospective patient visits Defendant's website, www.essentiahealth.org, to search for a doctor needed for a particular private treatment or condition, they may select the "Doctors & Providers" tab, which takes them to the "Find a Doctor or Provider Page." Below is a screenshot of the "Find a Doctor or Provider Page."

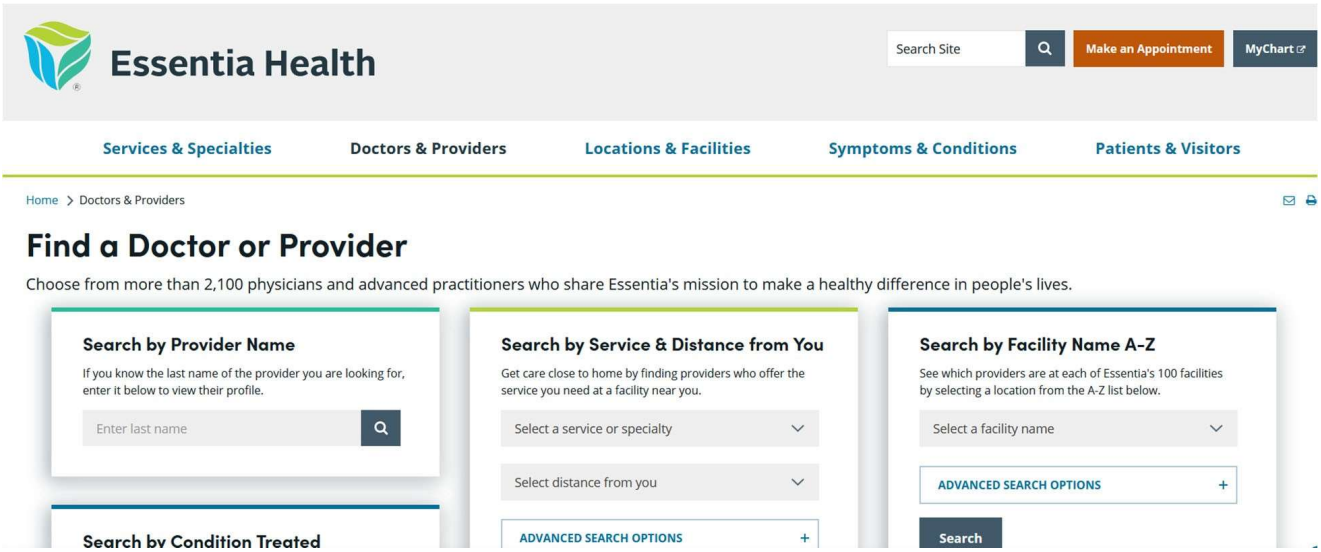


Figure 1. Defendant directs patients to its "Find a Doctor or Provider" webpage.

88. Because Defendant's website is embedded with Meta Pixel, the prospective patient 's communication when selecting the "Doctors & Providers" tab is automatically transmitted to Meta.

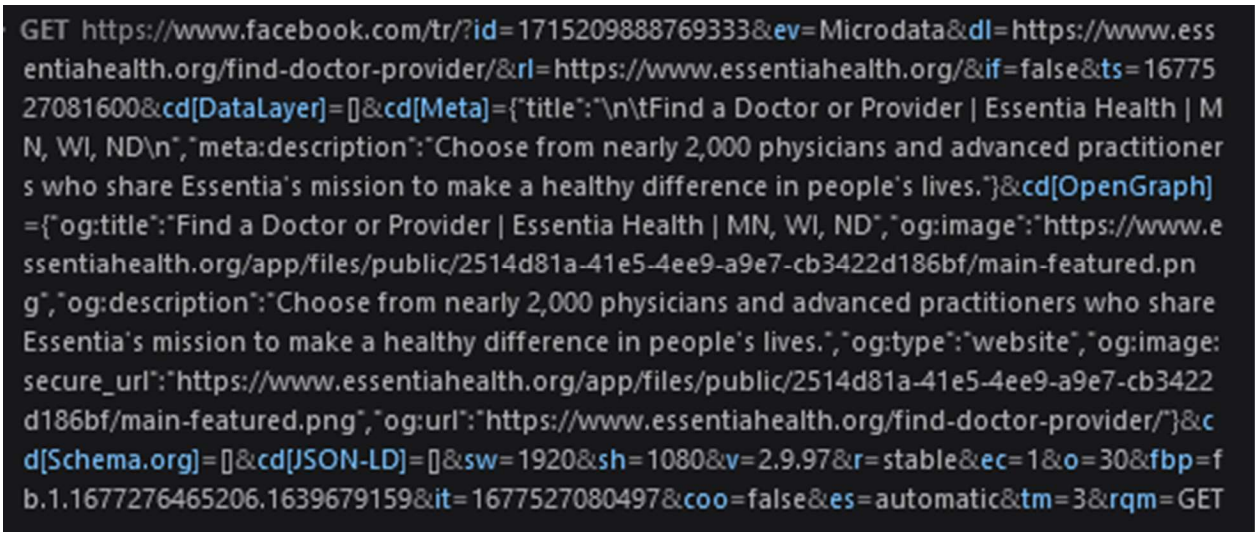


Figure 2. A screenshot of the Get Request via Firefox Web Developer demonstrating prospective patient 's communications related to finding a provider being shared with Meta. February 2023.

89. Defendant's website also allows patients to search for providers based on symptoms and conditions. For example, if the patient or prospective patient searches for a provider based upon a symptom or condition he will be prompted with the following screen.

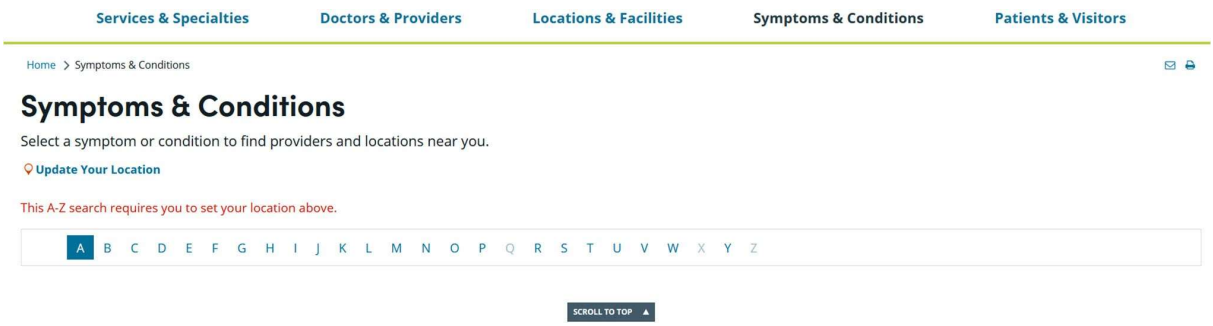


Figure 3. Defendant directs patients searching for a provider based on his symptoms or conditions to the "Symptoms & Conditions Page.

90. Before a patient can select a symptom or condition, the website requires the patient to enter location information, including a zip code, as noted in Figure 3 above. The prospective patient's location information is automatically transmitted to Meta.

Figure 4. A screenshot of the Get Request via Firefox Web Developer demonstrating Prospective patient 's location information being automatically transmitted to Meta: "MD, ND, WI." February 2023.

91. After inputting information, as required by Defendant, if a patient or prospective patient selects a symptom or condition from the "Symptoms & Conditions Page" or one of the pages associated therein the terms and phrases the patient or visitor selects are transmitted to Meta, even if they contain a prospective patient's private treatment, procedure, medical conditions, and related inquiries. This information is automatically sent from the prospective patient's device to Meta, and it reveals the individual's Facebook ID or other identifiers, along with each search filter the patient selected.

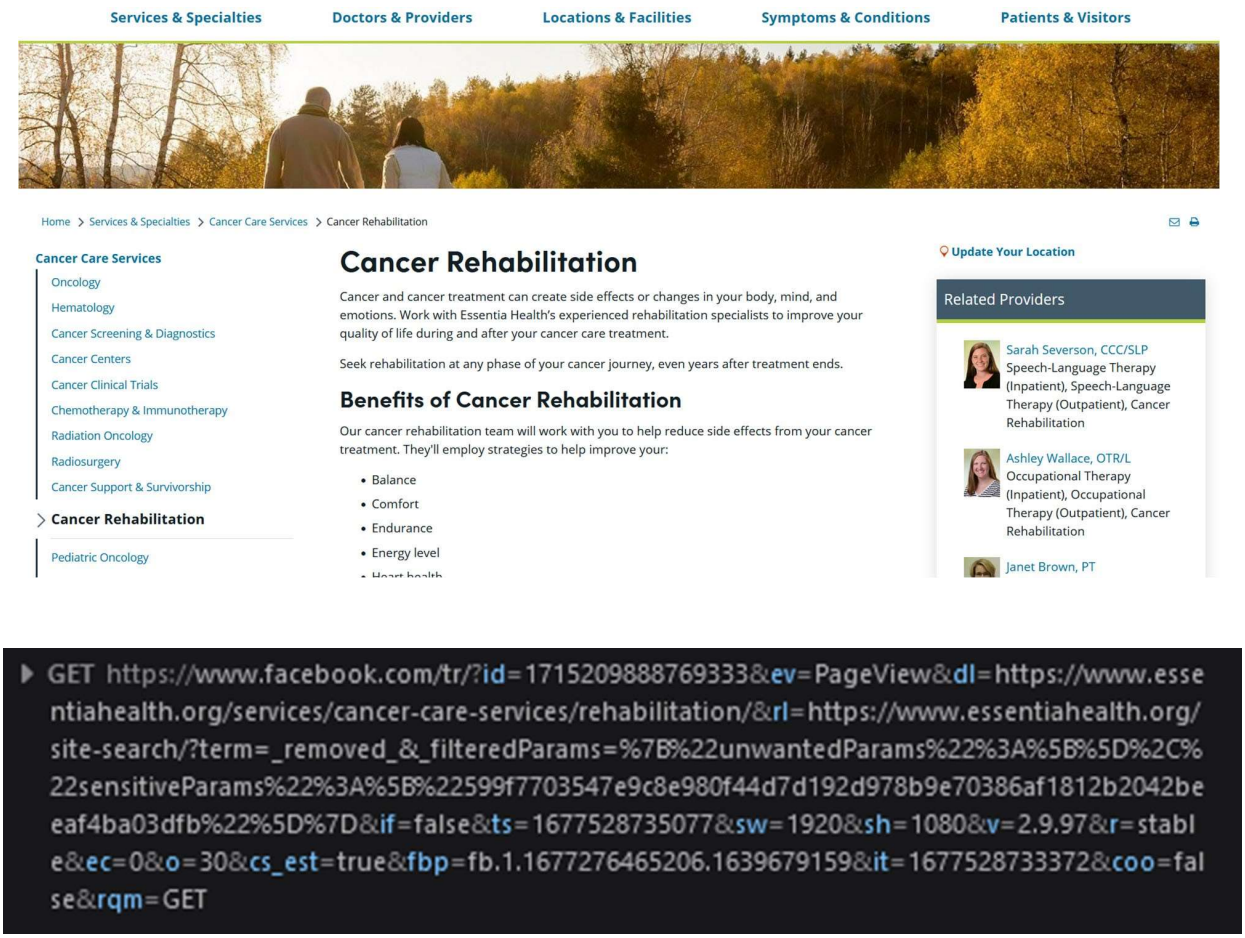


Figure 5. Example of search results for "Cancer Treatment" and selecting "Cancer Rehabilitation" from the results and a screen shot of the Get Request taken in Firefox Web Developer. February 2023.

92. Looking at the above Figures, it is clear Defendant's source code secretly instructs the prospective patient's browser to duplicate the visitor's communications and send those communications to Meta. This is also done with an identifier, so that the information can be linked to an actual person. This occurs in real-time.

93. Each time Defendant transmits this data to Meta, it also discloses the patient's personally identifiable information and information about their medical treatments, histories, and other inquiries. Additionally, each time a user who accesses Defendant's website while logged (or recently having logged) in, Facebook will transmit a cookie, or multiple cookies to Facebook, which contains that user's unencrypted Facebook ID. Defendant utilizes various cookies which can, in some instances, attach to a browser as a first-party cookie, identify a browser and a user, and disclose that information to Meta.[36]

94. Plaintiff and the Class members never consented, authorized, or otherwise permitted Defendant to disclose his personally identifiable and protected health information to third-parties, including Meta. Plaintiff was not provided with any prior written notice that Defendant disclosed his Website Communications, nor was she provided any means of opting out of such disclosures. Even so, Defendant knowingly and intentionally disclosed Plaintiff's and the Class members' protected and private information.

[36] Facebook.com, Cookies & OtherStorage Technologies, https://www.facebook.com/policy/cookies/ (last visited April 15, 2024).

E. Exposure of Sensitive Information Creates a Substantial Risk of Harm

95. The Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[37]

96. The FTC has also issued, and regularly updates, guidelines for businesses to implement reasonable data security practices and incorporate security into all areas of the business. According to the FTC, reasonable data security protocols require, among other things: (1) using industry tested and accepted methods; (2) monitoring activity on networks to uncover unapproved activity; (3) verifying that privacy and security features function properly; and (4) testing for common vulnerabilities or unauthorized disclosures.[38]

97. The FTC cautions businesses that failure to protect Sensitive Information and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money and patience to resolve the effect.[39] Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

---

[37] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022) https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf

[38] *Start With Security, A Guide for Business,* FTC (last visited Jan. 18, 2022) https://www.ftc.gov/business-guidance/resources/start-security-guide-business

[39] *See* Taking Charge, What to Do if Your Identity is Stolen, FTC, at 3 (2012) (last visited Jan. 19, 2022), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf

F. Plaintiff's and the Class Members' Sensitive Information is Valuable.

98. As many healthcare data industry experts have recognized, "[p]atients' medical data constitutes a cornerstone of the big data economy. A multi-billion-dollar industry operates by collecting, merging, analyzing and packaging patient data and selling it to the highest bidder."[40]

99. The personal, health, and financial information of Plaintiff and the Class is valuable and has become a highly desirable commodity. Indeed, one of the world's most valuable resources is the exchange of personal data.[41]

100. Business News Daily reported that businesses collect personal data (*i.e.*, gender, web browser cookies, IP addresses, and device IDs), engagement data (*i.e.*, consumer interaction with a business's website, applications, and emails), behavioral data (*i.e.*, customers' purchase histories and product usage information), and attitudinal data (*i.e.*, consumer satisfaction data) from consumers.[42] Companies then use this data to impact the customer experiences, modify their marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that may be even more lucrative.[43]

---

[40] Yaraghi, Niam, *Who should profit from the sale of patient data?,* The Brookings Institution, Nov. 19, 2018, https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/ (last visited March 18, 2023).

[41] *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[42] Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY (Aug. 5, 2022; updated Aug. 25, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[43] *Id.*

101. The power to capture and use customer data to manipulate products, solutions, and the buying experience is invaluable to a business's success. Research shows that organizations who "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25 percent in gross margin."[44]

102. In 2013, the Organization for Economic Cooperation and Development ("OECD") even published a paper entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value."[45] In this paper, the OECD measured prices demanded by companies concerning user data derived from "various online data warehouses."[46]

103. OECD indicated that "[a]t the time of writing, the following elements of personal data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., $2] for a date of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's license number and USD 35 for a military record. A combination of address, date of birth, social security number, credit record and military is estimated to cost USD 55."[47]

---

[44] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[45] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD Digital Economy Papers, NO. 220, OECD PUBLISHING PARIS, (Apr. 2, 2013), https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf.

[46] *Id.* at 25.

[47] *Id.*

104. Unlike financial information, such as credit card and bank account numbers, the PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are given at birth and attach to a person for the duration of his or his life. Medical histories are inflexible. For these reasons, these types of information are the most lucrative and valuable.[48]

105. Consumers place a considerable value on their Sensitive Information and the privacy of that information. One 2002 study determined that U.S. consumers highly value a website's protection against improper access to their Sensitive Information, between $11.33 and $16.58 per website. The study further concluded that to U.S. consumers, the collective "protection against error, improper access, and secondary use of personal information is worth between $30.49 and $44.62.[49] This data is approximately twenty years old, and the dollar amounts would likely be exponentially higher today.

106. Defendant's privacy violations exposed a variety of Sensitive Information, including medical histories, prescription information, communications with medical professionals, dates of birth, medical insurance information, and other highly sensitive data.

---

[48] *Calculating the Value of a Privacy Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy Enters, https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/ (last visited Jan. 18, 2022).

[49] 11-Horn Hann, Kai-Lung Hui, *et al*, *The Value of Online Information Privacy: Evidence from the USA and Singapore,* at 17. Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002), https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited Jan. 19, 2022).

107. It is important to note that the Social Security Administration ("SSA") warns that the unauthorized disclosure of a Social Security number can lead to identity theft and fraud.[50]

108. Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future.

109. PHI, like that exposed here, is likely even more valuable than Social Security numbers and just as capable of being misused.[51] PHI can be ten times more valuable than credit card information.[52] This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, social security numbers.[53]

110. Indeed, prescription records, blood tests, doctor notes, hospital visits and insurance records are all sold to commercial companies, which gather years of health

---

[50] Social Security Administration, *Identity Theft and Your Social Security Number*, (last visited Jan. 19, 2022), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[51] *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), https://publicintelligence.net/fbi-healthcare-cyber-intrusions/ (last visited Jan. 18, 2022).

[52] *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, Tim Greene, https://www.networkworld.com/article/2880366/anthem-hack-personal- data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 18, 2022).

[53] *Hackers Selling Healthcare Data in the Black Market*, INFOSEC, https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 18, 2022).

information on hundreds of millions of people and then sell it to other industries, like pharmaceutical companies who use the information to sell more drugs.[54] Some industry insiders and journalists are even calling hospitals the "brokers to technology companies" for their role in data sharing in the $3 trillion healthcare sector.[55] "Rapid digitization of health records … have positioned hospitals as a primary arbiter of how much sensitive data is shared."[56]

G. Plaintiff and the Class Members Had a Reasonable Expectation of Privacy in Their Interaction with Defendant's Website and Application.

111. Consumers are concerned about companies, like Defendant, collecting their data and assume the data they provide, particularly highly sensitive medical and insurance data, will be kept secure and private.

112. In a recent survey related to internet user expectations, most prospective patients stated they assume their detailed interactions with a website will only be used by the website and not be shared with a party they know nothing about.[57] As such, prospective patients reasonably expect that their interactions with a website should not be released to third parties unless explicitly stated.[58]

---

[54] Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Industry*, TIME, (Jan. 9, 2017), https://time.com/4588104/medical-data-industry/.
[55] Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, The Wall Street Journal, (Jan. 20, 2020), https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200.
[56] *Id.*
[57] *CUJO AI Recent Survey Reveals U.S. Internet Users Expectations and Concerns Towards Privacy and Online Tracking*, CUJO (May 26, 2020), https://www.prnewswire.com/news-releases/cujo-ai-recent-survey-reveals-us-internet-users-expectations-and-concerns-towards-privacy-and-online-tracking-301064970.html.
[58] Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A*

113. The majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.[59] In fact, the overwhelming majority of Americans equate personal privacy as important as concerns about crime, access to quality healthcare, and the future of the social security system.[60]

114. A recent study by Consumer Reports shows that 92% of Americans believe that internet companies and Website should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and Website should be required to provide consumers with a complete list of the data that has been collected about them.[61]

115. A March 2000 BusinessWeek/Harris Poll found that 89% of respondents were uncomfortable with web tracking schemes where data was combined with an individual's identity.[62] The same poll found that 63% of respondents were uncomfortable with web tracking even where the clickstream data was not linked to personally identifiable information.[63] A July 2000 USA Weekend Poll showed that 65% of respondents thought

---

Privacy Analysis, THE INFORMATION SOCIETY, 38:4, 257, 258 (2022).
[59] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.
[60] *Freedom of Information in the Digital Age*, AMERICAN SOCIETY OF NEWSPAPER EDITORS FREEDOM OF INFORMATION COMMITTEE AND THE FIRST AMENDMENT CENTER, (April 3, 2001).
[61] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumer-reports.org/consumerreports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.
[62] *Public Opinion on Privacy*, EPIC.ORG, https://archive.epic.org/privacy/survey/.
[63] *Id.*

that tracking computer use was an invasion of privacy.[64]

116. Patients and website users act consistently with their expectation of privacy. For example, following a new rollout of iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to allow such tracking.[65]

117. Like the greater population, certainly, Defendant's patients would expect the highly sensitive *medical* information they provided to Defendant, through the website or other applications, to be kept secure and private.

H. Defendant's Conduct Violated HIPAA

118. Under HIPAA, individuals' health information must be:

> properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Privacy Rule strikes a balance that permits important uses of information while protecting the privacy of people who seek care and healing.[66]

119. HIPAA is a "federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."[67] The rule requires appropriate administrative, physical, and

---

[64] *Id.*

[65] Margaret Taylor, *How Apple screwed Facebook*, WIRED, (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[66] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[67] *Health Insurance Portability and Accountability Act of 1996 (HIPAA),* Centers for Disease Control and Prevention (last visited Aug. 19, 2022) https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-

technological safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.[68]

120. HIPAA defines "individually identifiable health information" as including information that is (1) created or received by a health care provider, and (2) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past present, or future payment for the provision of health care to an individual, and which identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103.

121. Additionally, HIPAA defines sensitive patient personal and health information as: (1) Name; (2) Home and work addresses; (3) Home and work phone numbers; (4) Personal and professional email addresses; (5) Medical records; (6) Prescriptions; (7) Health insurance information; (8) Billing information; (9) Social Security number; (10) Spouse and children's information; and/or (11) Emergency contact information.[69]

122. To ensure protection of this private and sensitive health information, HIPAA mandates standards for handling PHI—the very data Defendant failed to protect. The Privacy violations described herein resulted from Defendant's failure to comply with

---

On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge

[68] U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[69] *What is Considered Protected Health Information Under HIPAA*, HIPAA Journal, Jan. 2, 2022: U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (last visited Aug. 19, 2022), https://www.hhs.gov/hipaa/forprofessionals/privacy/laws-regulations/index.html (last visited Aug. 19, 2022).

several of these standards:

a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits;

b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technological policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;

c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

d. Violation of 45 C.F.R. §164.306(a)(2): Failing to protect against any reasonably–anticipated threats or hazards to the security or integrity of electronic protected health information;

e. Violation of 45 C.F.R. §164.306(a)(3): Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

f. Violation of 45 C.F.R. §164.306(a)(94): Failing to ensure compliance with HIPAA security standard rules by its workforce;

g. Violation of 45 C.F.R. §164.502, *et seq*: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

h. Violation of 45 C.F.R. §164.530(c): Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information.

123. Moreover, according to Health and Human Services' Health Information Privacy Bulletin ("HHS Privacy Bulletin"), HIPAA covered entities cannot share PII or PHI to online tracking technology vendors for marketing purposes without first obtaining

the individual's HIPAA compliant authorization.[70] The HHS Privacy Bulletin explicitly states:

> The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.

HHS Privacy Bulletin (internal citations omitted) (emphasis in original).[71] This bulletin was updated as recently as March 18, 2024, and still reflects this language.

124. The HHS Privacy Bulletin also identifies several harms that may result from an impermissible disclosure of an individual's PHI, including:

> identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.

[70] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[71] *Id.*

HHS Privacy Bulletin (internal citations omitted)(emphasis in original).[72] This bulletin was updated as recently as March 18, 2024, and still reflects this language.

125. According to HHS, HIPAA "[r]egulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website, including individually identifiable health information that the individual provides when they use regulated entities' websites." The information an individual provides may include a medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code.[73] The HHS Privacy Bulletin considers HIPAA Rules to apply to tracking on both user authenticated and unauthenticated webpages. [74]

126. Furthermore, under 42 U.S.C. § 1320d-6, HIPAA criminalizes the "use[] or cause[] to be used a unique health identifier" or to "disclose[] individually identifiable health information to another person . . . without authorization" from the patient. Where a violation of § 1320d-6 is "committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm," the penalty is enhanced. *Id.*

127. All of the above listed information that is collected on a regulated entity's website, like Defendant's website, is PHI, "even if the individual does not have an existing

---

[72] *Id.*
[73] *Id.*
[74] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, (Mar. 18, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. (last visited Apr. 16, 2024).

relationship with the regulated entity and even if the [information], such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services." When a regulated entity, again like Defendant, collects the individual's information, that information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[75]

CLASS ALLEGATIONS

128. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23 on behalf of themselves and all others similar situated, as representative of the following Class:

> All persons whose Sensitive Information was disclosed to a third party through Defendant's Website without authorization or consent.

129. Excluded from the Class are Defendant; its officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

130. Plaintiff reserves the right to modify and/or amend the Class definition, including but not limited to creating additional subclasses, as necessary.

131. All members of the proposed Class are readily identifiable through

[75] *Id.*

Defendant's records.

132. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes at least 1.5 million people. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

133. **Commonality and Predominance.** This action involves common questions of law and fact to the Plaintiff and Class members, which predominate over any questions only affecting individual Class members. These common legal and factual questions include, without limitation:

a. Whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their Sensitive Information;

b. Whether Defendant owed Plaintiff and the other Class members a duty to secure their Sensitive Data from third-party tracking technologies provided by Meta;

c. Whether Defendant owed Plaintiff[s] and the other Class members a duty to implement reasonable data privacy protection measures because Defendant accepted, stored, created, and maintained highly sensitive information concerning Plaintiff and the Class;

d. Whether Defendant knew or should have known of the risk of disclosure of data through third party tracking technologies;

e. Whether Defendant breached its duty to protect the Sensitive Information of Plaintiff and other Class members;

f. Whether Defendant knew or should have known about the inadequacies of its privacy protection;

g. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized disclosure;

h. Whether proper data security measures, policies, procedures and protocols were enacted within Defendant's offices and computer systems to safeguard and protect Plaintiff's and the Class's Sensitive Information from unauthorized disclosure;

i. Whether Defendant's conduct was the proximate cause of Plaintiff's and the Class's injuries;

j. Whether Plaintiff and the Class suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;

k. Whether Plaintiff and the Class are entitled to recover damages; and

l. Whether Plaintiff and the Class are entitled to other appropriate remedies including injunctive relief.

134. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of himself and the Class. Individual questions, if any, are slight by comparison in both quality and quantity to the common questions that control this action.

135. **Typicality.** Plaintiff's claims are typical of those of other Class members because Plaintiff's Sensitive Information, like that of every other Class member, was improperly disclosed by Defendant. Defendant's misconduct impacted all Class members in a similar manner.

136. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interest of the members of the Class and has retained counsel experienced in complex consumer class action litigation and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

137. **Superiority.** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. The damages or other financial

detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court.

CLAIMS

COUNT I
VIOLATIONS OF ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), 18 U.S.C. § 2511, *et seq.*
(On behalf of Plaintiff and the Nationwide Class)

138. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

139. The ECPA protects against intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1).

140. The ECPA further provides any person who

> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

18 U.S.C. § 2511(1)(c) & (d).

141. Pursuant to 18 U.S.C. § 2511(5)(b), for violations of the ECPA, the Court "may use any means within its authority to enforce an injunction issued under paragraph (ii)(A) and shall impose a civil fine of not less than $500 for each violation of the injunction. Additionally, 18 U.S.C. § 2520 provides that "any person whose wire, oral or electronic communication is intercepted, disclosed or intentionally used in violation of Chapter 119, may recover from the person or entity that engaged in the violation in a civil action.

142. The transmission of Plaintiff's and the Class members' Sensitive Information from Essentia's website to Meta violates the ECPA. First, the transmissions from Plaintiff and the Class members to Defendant, through Defendant's Website (www.essentiahealth.org or www.essentiahealth.org/MyChart) are communications pursuant to 18 U.S.C. § 2510(12).

143. "Interception" means "the acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents… include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C.§ 2510(4), (8).

144. "Content" means "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." U.S.C.§ 2510(8).

145. "Intercepting device" or the "Electronic, mechanical or other device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication. U.S.C.§ 2510(5). Here, Plaintiff's and the Class members' browsers and computing devices and Defendant's webservers, website, and the Pixel code Defendant deployed are all "devices" for the purposes of the ECPA.

146. "Electronic communication" means *any communication* made in whole or in part through the use of facilities for the transmission of communications by the signs, signals, writing or data between the point of origin and the point of reception. U.S.C.§ 2510(2).

147. By employing and embedding Pixel on Defendant's website, Defendant intentionally violated the ECPA, through its interception, attempt at interception, and its procurement of Meta to intercept the electronic communications of Plaintiff and the Class members.

148. Under the ECPA, even a party to a communication violates the act by "intercept[ing] a wire, oral, or electronic communication . . . for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.* at § 2511(d).

149. Even as a party to the communication, Essentia violated the ECPA because it intercepted or caused to be intercepted communications for " the purpose of committing [a] criminal or tortious act[.]" Specifically, Essentia permitted the interception of communications with its website by Meta for the express purpose of using that private, medical information to subsequently craft and display advertisements for Essentia (and

Meta's) profit and to increase Essentia's reach and exposure to potential patients.

150. Under HIPAA, however, such conduct is criminal. That is, 42 U.S.C. § 1320d-6 states that it is a criminal violation to "use[] or cause[] to be used a unique identifier" or to "disclose[] individually identifiable health information to another person . . . without authorization[.]" Where that private information is disclosed "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm", the penalty for violating § 1320d-6 is enhanced.

151. That is precisely what occurred here. Essentia intercepted and disclosed Plaintiff's and the Class's communications to Meta without authorization for financial gain, particularly, to use that private information to craft targeted ads to increase its revenue. As such, Essentia and Meta's interception of Plaintiff's communications with Essentia's website were for the express purpose of profiting in violation of 42 U.S.C. § 1320d-6.

152. Essentia's conduct also violated Minnesota law. Under Minn. Stat. § 609.891, a person is guilty of a crime if the person "intentionally and without authorization attempts to or does penetrate a computer security system or electronic terminal." Here, Essentia intentionally and without authorization breached Plaintiff's and the Class's web browsers to secretly install Meta's Pixel code that then monitored and collected all their website activity.

153. By disclosing confidential information, Essentia also violated Minn. Stat. § 144.651, the Minnesota Health Care Bill of Rights, and Minn. Stat. § 144.291, the Minnesota Health Records Act. Under § 144.651, subd. 15 and 16, patients have the right

to privacy concerning their treatment and the confidentiality of their medical records. Under § 144.291, patient consent is required to release their medical records. By inviting Meta to spy on Plaintiff's interactions with Essentia's website, Essentia shared Plaintiff's and the Class's private medical information with a third party and without authorization.

154. Consequently, Essentia accessed, obtained, and disclosed Plaintiff's and Class's Sensitive Information for the purpose of committing the crimes and torts described herein, and did so because it would not have been able to obtain or use the information or the marketing services if it had complied with the law without violating federal and state law.

155. At no time did Plaintiff and the Class members provide their consent to Defendant's disclosure of their Sensitive Information to Meta and/or other third-parties. Further, Defendant has improperly profited from its invasion of Plaintiff's and the Class members' privacy in its use of their data for its economic value.

156. Plaintiff and the Class members are entitled to damages, including compensatory and/or nominal damages in an amount to be proven at trial.

157. To the extent Defendant's conduct is ongoing, and it continues to unlawfully disclose the communications of Plaintiff and the Class members any time they use or provide information to Defendant through its Website or application without their consent, Plaintiff and the Class members are entitled to declaratory and injunctive relief. This will prevent future unlawful and unauthorized disclosure of Plaintiff's and the Class members' Sensitive Information.

COUNT II
VIOLATION OF MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT ("MUDTPA") § 325D.43-48
(On behalf of Plaintiff and the Nationwide Class)

158. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

159. Defendant is subject to the rules and statutory requirements of Minn. Stat. § 325D.44, because it advertised, offered, or sold goods or services in Minnesota and therefore engaged in business directly or indirectly affected people in Minnesota.

160. The MDUTPA prohibits deceptive trade practices in person's business, vocation, or occupation, *See* Minn. Stat. § 325D.44, subd. 1, including where the person:

> represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that the person does not have; Minn. Stat. § 325D.44, subd.1(5).
>
> represents that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; Minn. Stat. § 325D.44, subd.1(7).

161. Defendant engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Sections Minn. Stat. § 325D.44, subd. 1(5) & (7).

162. Defendant's representations and omissions include both implicit and explicit representations through:

a. Failing to implement and maintain reasonable privacy measures to protect Plaintiff's and the Class's Sensitive Information, which was a direct and proximate cause of the Privacy violations described herein;

b. Failing to identify and remediate foreseeable privacy risks and

adequately maintain privacy measures despite knowing the risk disclosure of patients' Sensitive Information, which was a direct and proximate cause of the Privacy violations;

c. Failing to comply with common law and statutory duties pertaining to the privacy of Plaintiff's and the Class's Sensitive Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.102 and the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Privacy violations;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class's Sensitive Information, including by implementing and maintaining reasonable privacy protection measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the privacy of Plaintiff's and Class's Sensitive Information, including duties imposed by the HIPAA, 45 C.F.R. § 160.102;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately protect Plaintiff's and Class's Sensitive Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class's Sensitive Information, including duties imposed by HIPAA, 45 C.F.R. § 160.102 or the FTC Act, 15 U.S.C. § 45.

163. Defendant's acts and practices were "unfair" because they caused or were likely to cause substantial injury to patients which was not reasonably avoidable by patients themselves and not outweighed by countervailing benefits to patients or to competition.

164. The injury to patients from Defendant's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Sensitive Information.

165. Plaintiff and the Class could not have reasonably avoided injury because Defendant's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of patient healthcare decision-making and information gathering. By withholding important information from patients about the inadequacy of its privacy protections and Defendant's intentional use of Pixel on its website, Defendant created an asymmetry of information between it and patients that precluded patients from taking action to avoid or mitigate injury.

166. Defendant also engaged in "deceptive" acts and practices in violation of Minn. Stat. § 325D.44, including:

> 1. Misrepresenting that the subject of a consumer transaction has performance, characteristics, or benefits it does not have which the supplier knows or should reasonably know it does not have; and
> 2. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not.

167. Specifically, Defendant made the following misrepresentations, as stated previously herein:

> 1. Defendant tells patients it will keep their sensitive Information secure and private. Indeed, Defendant represents that it is committed to doing what's right by following the highest business ethical standards. It states that it will comply with all applicable laws and regulations as well as our own internal policies and procedures. *See supra*, ¶ 29.
> 2. Essentia maintains a "Health Code of Integrity" in which it commits to "avoiding injuries to patients from the care that is intended to help them," "doing the right thing," "complying with laws, regulations, and applicable Essentia Health policies and procedures," "comply[ing] with various federal, state, and local laws and regulations that are in place to safeguard our patients and our organization," and "to provide the quality care reflected in recognized professional standards." *See supra,* ¶ 30.

> 3. Essentia also maintains a Privacy Policy through which it states. "Essentia Health is committed to protecting the privacy of those who visit our website." *See supra*, ¶ 31.

168. Plaintiff and the Class had a reasonable expectation of privacy and relied on Defendant to protect the Sensitive Information provided to it and created by it, especially because, medical facilities are always required to maintain confidentiality of patient records, with very limited exceptions.

169. Defendant knew or should have known that failing to adequately protect patient information could cause substantial harm. Moreover, through its various policies, Defendant acknowledged its obligation to reasonably safeguard sensitive information against unauthorized disclosure of Sensitive Information to third-parties like Meta.

170. Had Defendant disclosed to Plaintiff and the Class that it used Meta Pixel which publicly disclosed sensitive, medical information, Defendant would have been unable to continue this type of business practice and it would have been forced to adopt reasonable data privacy measures and comply with the law. Defendant was trusted with sensitive and valuable PII and PHI regarding millions of patients, including Plaintiff and the Class. Defendant accepted the responsibility of protecting the data while keeping the state of the tracking technologies used on its site and application secret from the public. Accordingly, Plaintiff and the Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

171. Defendant had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the PII and PHI in its possession, and the generally accepted professional standards. This duty arose due to the

representations and relationship between Defendant and Plaintiff and the Class as described herein. Defendant had exclusive or superior knowledge of the practices engaged in where private information related to health and safety was shared with third-parties which Plaintiff and the members of the class had no reasonable manner of obtaining in advance, giving rise to a further duty to disclose.

172. As a direct and proximate result of Defendant's unfair, abusive, and deceptive acts or practices, Plaintiff and the Class have suffered and will continue to suffer injury and monetary damages, as described herein, including but not limited to; loss of value of their PII and PHI; overpayment for Defendant's services, and the deliberate violation of their privacy as alleged herein.

173. Plaintiff and the Class seek all relief allowed by law, including injunctive relief, costs and attorneys' fees, and remedies cumulative.

COUNT III
VIOLATION OF THE MINNESOTA WIRETAP STATUTE
Chapter 626A.02
(On behalf of Plaintiff and the Nationwide Class)

174. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

175. The Minnesota Wiretap Statute, Minn. Stat. 626A, protects against intentional interception, attempted interception, or the procurement of another person to intercept or attempt to intercept any wire, oral, or electronic communication. *See* Minn. Stat. 626A.02, Subd. 1.

176. The Minnesota Wiretap Statute further provides any person who

> (2) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
>
> > (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
> > (ii) such device transmits communications by radio, or interferes with the transmission of such communication;
>
> (3) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> (4) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
>
> Shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

Minn. Stat. 626A.02.

177. Additionally, a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of Chapter 626A may recover from the person or entity that engaged in violation:

> 1. Temporary and other equitable or declaratory relief as may be appropriate;
> 2. Damages under subd. 3 …; and
> 3. A reasonable attorney's fee and other litigation costs reasonable incurred.

Minn. Stat. 626A.13, Subd. 2

178. The transmission of Plaintiff's and the Class members' Sensitive Information violates the Minnesota Wiretap Act. First, the transmissions from Plaintiff and the Class members to Defendant, through Defendant's Website (www.essentiahealth.org or www.essentiahealth.org/MyChart) are wire communications pursuant to Minn. Stat. 626A.01, Subd. 3.

179. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." Minn. Stat. 626A.01, Subd. 5.

180. "Contents" means "when used with respect to any wire, electronic, or oral communication, includes any information concerning the substance, purport, or meaning of that communication." Minn. Stat. 626A.01, Subd. 8.

181. "Electronic, mechanical or other device" means any device or apparatus which can be used to intercept a wire, electronic, or oral communication. Minn. Stat. 626A.01, Subd. 6. Here, Plaintiff's and the Class members' browsers and computing devices and Defendant's webservers, website, and the Pixel code Defendant deployed are all "devices" for the purposes of the Minnesota Wiretap Statute.

182. "Electronic communication" means transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system but does not include:

(1) a wire or oral communication;

(2) a communication made through a tone-only paging device; or

(3) a communication from a tracking device, defined as an electronic or mechanical

device which permits the tracking of the movement of a person or object.

Minn. Stat. 626A.01, Subd. 14.

183. By employing and embedding Pixel on Defendant's website, Defendant intentionally violated the Minnesota Wiretap Statute, through its interception, attempt at interception, and its procurement by Meta to intercept the electronic communications of Plaintiff and the Class members.

184. Indeed, Defendant willfully used or attempted to use the contents of Plaintiff's and the Class members' electronic communications, knowing that the information was obtained through interception.

185. Under the Minnesota Wiretap Statute, even a party to a communication violates the act by "intercept[ing] a wire, oral, or electronic communication . . . for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." Minn. Stat. 626A.02, Subd. 2(d).

186. Even as a party to the communication, Essentia violated the Minnesota Wiretap Act because it intercepted or caused to be intercepted communications for " the purpose of committing [a] criminal or tortious act[.]" Specifically, Essentia permitted the interception of communications with its website by Meta for the express purpose of using that private, medical information to subsequently craft and display advertisements for Essentia (and Meta's) profit and to increase Essentia's reach and exposure to potential patients.

187. Under HIPAA, however, such conduct is criminal. That is, 42 U.S.C. § 1320d-6 states that it is a criminal violation to "use[] or cause[] to be used a unique

identifier" or to "disclose[] individually identifiable health information to another person . . . without authorization[.]" Where that private information is disclosed "with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm", the penalty for violating § 1320d-6 is enhanced.

188. That is precisely what occurred here. Essentia intercepted Plaintiff's and the Class's communications to Meta without authorization for financial gain, particularly, to use that private information to craft targeted ads to increase its revenue. As such, Essentia and Meta's interception of Plaintiff's communications with Essentia's website were for the express purpose of profiting in violation of 42 U.S.C. § 1320d-6.

189. Essentia's conduct also violated Minnesota law. Under Minn. Stat. § 609.891, a person is guilty of a crime if the person "intentionally and without authorization attempts to or does penetrate a computer security system or electronic terminal." Here, Essentia intentionally and without authorization breached Plaintiff's and the Class's web browsers to secretly install Meta's Pixel code that then monitored and collected all their website activity.

190. By disclosing confidential information, Essentia also violated Minn. Stat. § 144.651, the Minnesota Health Care Bill of Rights, and Minn. Stat. § 144.291, the Minnesota Health Records Act. Under § 144.651, subd. 15 and 16, patients have the right to privacy concerning their treatment and the confidentiality of their medical records. Under § 144.291, patient consent is required to release their medical records. By inviting Meta to spy on Plaintiff's interactions with Essentia's website, Essentia shared Plaintiff's and the Class's private medical information with a third party and without authorization.

191. Consequently, Essentia accessed, obtained, and disclosed Plaintiff's and Class's Sensitive Information for the purpose of committing the crimes and torts described herein, and did so because it would not have been able to obtain or use the information or the marketing services if it had complied with the law without violating federal and state law.

192. At no time did Plaintiff and the Class members provide their consent to Defendant's disclosure of their Sensitive Information to Meta and/or other third-parties.

193. Further, Defendant has improperly profited from its invasion of Plaintiff's and the Class members' privacy in its use of their data for its economic value.

194. Plaintiff and the Class members are entitled to damages, including compensatory and/or nominal damages in an amount to be proven at trial.

195. To the extent Defendant's conduct is ongoing, and it continues to unlawfully disclose the communications of Plaintiff and the Class members any time they use or provide information to Defendant through its Website or application without their consent, Plaintiff and the Class members are entitled to declaratory and injunctive relief. This will prevent future unlawful and unauthorized disclosure of Plaintiff's and the Class members' Sensitive Information.

196. Pursuant to Minn. Stat. 626A.13, Subd. 3, the Court may assess damages by (1) the sum of three times the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, whichever is greater of option (1) and option (2).

197. As a direct and proximate result of Defendant's conduct and pursuant to the Minnesota Wiretap Act, the Court may assess statutory damages; preliminary and other equitable or declaratory relief as may be appropriate; and reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT IV
Violation of the Minnesota Health Records Act Minn. Stat. §§ 144.291 and 144.293
(On Behalf of the Plaintiff and the Nationwide Class)

198. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

199. Under the Minnesota Health Records Act ("MHRA"), "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of healthcare to a patient; or the past, present, or future payment for the provision of healthcare to a patient. Minn. Stat. § 144.291, subd. 2(c).

200. The information Plaintiff and the Class members exchanged with Defendant on its website concerned the past, present, and future physical or mental health or condition and the provision of healthcare. Specifically, Plaintiff has included allegations related to information and exchanges on Defendant's website that disclosed his specific health care providers, including Dr. Daniel Nikcevich in or around February 2022 and Dr. Nahi Kiblawi, and specific conditions, including bladder cancer, sleep apnea, and diabetes and treatments for those conditions. Thus, that information constitutes "health records" as that term is defined in the MHRA.

201. Plaintiff and the Class members are "patients" at all relevant times as that term is defined under the MHRA. Minn. Stat. § 144.291, subd. 2(g).

202. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

203. Defendant's use of Meta Pixel, Defendant resulted in Defendant providing a third party with Plaintiff's and the Class member's health records and, furthermore, allowed a third party to access, without authorization, Plaintiff's and the Class members' health records.

204. Neither Plaintiff nor the Class members consented to or otherwise authorized Defendant to share their health records with Meta or any other third-party.

205. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees. Minn. Stat. § 144.298, subd. 2. As a result of Defendant's violations of the MHRA, Plaintiff and the other Class members seek all damages authorized by law, including compensatory damages plus costs, and reasonable attorney fees.

COUNT V
VIOLATION OF THE MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. § 325F.69 *et seq*
(On behalf of Plaintiff and the National Class)

206. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

207. Defendant's practices were and are in violation of Minnesota's Consumer Fraud Act, Minnesota Statutes § 325F.69, *et seq.*

208. Defendant is a person as defined by Minnesota Statute § 325F.68, subd. 3.

209. The medical services that Defendant markets, provides, offers and/or sells are considered merchandise. Minnesota Statute §325F.69, Subd. 2.

210. As alleged, Defendant engaged in deceptive acts and practices in the form of misrepresentations and omissions while conducting business throughout Minnesota to thousands of individuals seeking medical care. Specifically, Defendant represented that it lawfully, and in accordance with healthcare standard practices, protected the confidentiality and privacy of its patients and also omitted material information regarding its use of Meta Pixel on its website to the public at large. Defendant did not protect the confidentiality or privacy of its patients and it does in fact use Meta Pixel on its website which the general public can access online.

211. Defendant did not disclose its use of the Meta Pixel on its website or that it was sharing private, sensitive patient data with the third-party Meta without patients' consent. Defendant's failure to inform patients or potential patients of its use of Meta

Pixel on its website and its disclosure of patient and website visitors' data to third parties was likely to, and did deceive Plaintiff and the Class members.

212. As a direct result of Defendant's unlawful deceptive practices, Plaintiff and the Class members suffered injuries including the loss of their personal, private data.

213. Plaintiff and the Class members seek an award of damages for violations of Minn. Stat. § 325.69 pursuant to Minn. Stat. § 8.31, subd. 3a and all other appropriate relief.

COUNT VI
UNJUST ENRICHMENT
(On behalf of Plaintiff and the National Class)

214. Plaintiff realleges and incorporates by reference every allegation contained in the paragraphs above as though fully stated herein.

215. Plaintiff and the Class members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare related information and knowledge. Defendant receives a benefit from its use of Plaintiff's and the Class members' Sensitive Information, including monetary compensation and savings. Defendant intentionally collected and used Plaintiff's and the Class members' Sensitive Information for its own gain, without consent or authorization.

216. Defendant unjustly retained those benefits, which include savings on marketing and increased profits, at the expense of Plaintiff and the Class members and this conduct damaged Plaintiff and the Class members. Plaintiff and the Class members were not compensated by Defendant for the data they provided.

217. It would be inequitable and unjust for Defendant to retain any of the profit or other benefits derived from the secret, unfair, and deceptive data tracking methods Defendant employes on www.essentiahealth.org.

218. The Court should require Defendant to disgorge all unlawful or inequitable proceeds that it received into a common fund for the benefit of Plaintiff and the Class members, and order other such relief as the Court may deem just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment in his favor as follows:

a. Certification the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;

b. Designation of Plaintiff as representative of the Class and the undersigned counsel as Class Counsel;

c. An award of damages in an amount to be determined at trial or by this Court;

d. An order for injunctive relief, enjoining Defendant from engaging in the wrongful and unlawful acts described herein;

e. An award of statutory interest and penalties;

f. An award of costs and attorneys' fees; and

g. Such other relief the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully submitted,

Dated: April 19, 2024

/s/ Brian C. Gudmundson

Brian C. Gudmundson, (#336695)
Jason P. Johnston, (#391206)
Michael J. Laird, (#398436)
Rachel K. Tack, (#399529)
Benjamin R. Cooper, (#403532)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com
jason.johnston@zimmreed.com
michael.laird@zimmreed.com
rachel.tack@zimmreed.com
benjamin.cooper@zimmreed.com

Hart L. Robinovitch, (#240515)
ZIMMERMAN REED LLP
14648 N. Scottsdale Road., Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
hart.robinovitch@zimmreed.com

Nathan D. Prosser, (#0329745)
Anne T. Regan, (#0333852)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 522-4291
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

Daniel E. Gustafson, (#202241)
Karla M. Gluek, (#238399)
David A. Goodwin, (#386715)
Anthony J. Stauber, (#401093)
GUSTAFSON GLUEK PLLC
Canadian Pacific Plaza
120 South 6th Street, Suite 2600
Minneapolis, MN 55402

Telephone: (612) 333-8844
dgustafson@gustafsongluek.com
kgluek@gustafsongluek.com
dgoodwin@gustafsongluek.com
tstauber@gustafsongluek.com

Attorneys for Plaintiff